ANALISI QUALITATIVA

INTRODUZIONE

La sezione qualitativa propone una serie di contributi autorevoli curati da docenti universitari, imprenditori, magistrati, avvocati, consulenti informatici forensi, giornalisti e più in generale professionisti che si sono distinti nel panorama legal tech italiano. Ogni contributo offre un punto di vista inedito sullo stato dell'arte e le prospettive del settore, con suggestive previsioni di medio periodo.

Non è stato chiesto agli autori di trattare uno specifico argomento e non è nemmeno stato fornito un dettaglio di quanto prodotto dai colleghi. Questo ha permesso di ottenere un contributo neutro, libero da vizi di forma e contenuto.
Abbiamo così trasformato la ridondanza in una linea guida, un segnale del fatto che certi argomenti, più di altri, sono al momento sotto i riflettori e hanno raccolto l'interesse e l'attenzione di molteplici professionisti.

Per ogni contributo abbiamo predisposto uno o più "focus box" che, a nostro avviso, raccolgono gli spunti più incoraggianti ma anche le perplessità che caratterizzano questo particolare settore, più di altri, refrattario al cambiamento. Così facendo anche il lettore più avido di stimoli immediati potrà contare su un secondo livello di lettura veloce.

IL DIBATTITO SULLA FAIR SHARE E CENNI SUI POSSIBILI RIFLESSI PRATICI

Filippo Alberti, Freshfields Bruckhaus Deringer

Le modalità di svolgimento di molte attività professionali (tra cui quelle di aziende e consulenti legali) stanno progressivamente cambiando. Ciò anche grazie al sempre maggior utilizzo di soluzioni tecnologiche divenute oramai pressoché indispensabili; si pensi, ad esempio, ai sistemi di videoconferenza che consentono agevolmente l'organizzazione di riunioni tra persone fisicamente distanti, la partecipazione da remoto ad udienze, ecc.

In questo contesto, si inserisce anche l'annoso dibattito sulla c.d. Fair Share, che non può e non deve ridursi, dunque, meramente ad una "guerra dei mondi" tra operatori telefonici e di rete (ISP), da un lato, e, dall'altro, big tech, ma si estende e coinvolge una vasta pluralità di attori e soggetti interessati, tra cui, ad esempio e in aggiunta alle già citate big tech, OTT players, fornitori di videogiochi online e di servizi digitali, ivi comprese, per l'appunto, le piattaforme per riunioni in via telematica (complessivamente, i c.d. CAP).

La questione verte sostanzialmente intorno all'interrogativo se – e, nel caso, in quale misura – le società che forniscono servizi che comportano una significativa trasmissione dati (i CAP) debbano contribuire ai costi per lo sviluppo della rete degli ISP (e quali possano essere le possibili implicazioni delle varie soluzioni). Non può, quindi, non cogliersi il rilievo che l'individuazione di una strategia di policy, in un senso o nell'altro, potrebbe avere anche sulla fruizione e messa a disposizione di soluzioni tecnologiche in svariati campi, tra cui quelli in cui ci troviamo ad operare.

La tematica in oggetto ha portata mondiale e, negli ultimi mesi, ha (ri)acceso la discussione a livello europeo, a seguito della consultazione pubblica avviata dalla Commissione Europea a febbraio 2023 nell'ambito del più ampio pacchetto "Gigabit".

A cascata, i singoli Stati Membri hanno aderito a posizioni diverse. L'Italia (e, in particolare, l'AGCom, in seno al BEREC), pur non essendosi ancora del tutto schierata, non si è mostrata, allo stato, del tutto convinta delle ragioni sottese al testo proposto in consultazione dalla Commissione Europea.

La sensazione è che, nonostante le innumerevoli dichiarazioni pubbliche e positioning paper in materia, le valutazioni al riguardo siano ancora ad uno stato embrionale e che un eventuale sviluppo non possa prescindere dalla disamina quantomeno di alcune questioni principali che verranno accennate brevemente qui di seguito.

«Si tenga presente che il – invero, piuttosto generale – testo posto in consultazione dalla Commissione Europea prevede essenzialmente due modelli applicativi: il primo, per l'appunto, assimilabile ad un contributo diretto dei CAP in favore degli ISP e un secondo concepito come la creazione di un fondo alimentato dai CAP a cui gli ISP attingerebbero per sostenere gli investimenti necessari alla realizzazione o miglioramento delle infrastrutture di rete.»

Anzitutto, sembrerebbe dirimente stabilire se sia effettivamente in atto un fallimento di mercato (a principale pregiudizio degli ISP) tale da giustificare un intervento pubblico dell'economia con l'introduzione di un contributo (a detta di alcuni, assimilabile ad una tassa) a regolazione del mercato stesso.

Assumendo – per esigenze illustrative – che la risposta al precedente quesito sia affermativa, sorge un altro non trascurabile interrogativo, ossia come dovrebbe essere parametrato tale contributo, sia in termini quantitativi (banalmente, a quanto dovrebbe ammontare), sia in termini qualitativi (a quali parametri verrebbe ancorato).

Si tenga presente che il – invero, piuttosto generale – testo posto in consultazione dalla Commissione Europea prevede essenzialmente due modelli applicativi: il primo, per l'appunto, assimilabile ad un contributo diretto dei CAP in favore degli ISP e un secondo

concepito come la creazione di un fondo alimentato dai CAP a cui gli ISP attingerebbero per sostenere gli investimenti necessari alla realizzazione o miglioramento delle infrastrutture di rete. Va detto che non è neppure agevole trarre qualche spunto dall'applicazione di strumenti analoghi in altri Paesi od ordinamenti, dal momento che sono pochi gli esempi di posa in essere di un simile meccanismo e, per giunta, si tratta spesso di casi che hanno dato luogo ad estenuanti contenziosi o che, comunque, come, ad esempio, in Corea del Sud, non sembrano aver riscontrato i risultati sperati.

Con riferimento poi all'identità dei CAP, non è chiaro chi verrebbe fatto rientrare in tale categoria, atteso che qualsiasi scelta compiuta in tal senso rischierebbe di risultare discriminatoria per qualcuno. Il che non sarebbe privo di effetti, dal momento che, già di per sé, l'imposizione (o meno) della "tassa" in questione potrebbe avere un impatto significativo sul livello degli investimenti dei singoli operatori (visto, peraltro, anche il grado di interdipendenza – per alcuni, quasi simbiotico – delle attività economiche rispettivamente svolte), a nocumento, in ultima istanza, dei consumatori finali, oltre che della garanzia del rispetto del c.d. net neutrality principle.

Peraltro, proprio in Italia, si è recentemente assistito all'emergere di una problematica per certi versi riconducibile alla declinazione in concreto del concetto di Fair Share[1], che, tuttavia, ha trovato soluzione con un intervento ad hoc delle autorità competenti (in particolare, dell'AGCom), prediligendo, dunque, l'adozione di misure regolatorie concrete e specifiche, che sembrerebbero poter ovviare all'assenza di un sistema di "prelievo fiscale", quale quello del Fair Share.

In conclusione, si tratta senza dubbio di un tema di grande ed attuale interesse, atteso che i riflessi che ne deriveranno, in concreto, saranno via via sempre maggiore. Ad oggi, lo stato della discussione è ancora ferma ad uno scambio reciproco di accuse di free riding (i CAP "sfruttano" sempre più le reti degli ISP a scapito di quest'ultimi, ancorché gli stessi ISP traggono, in qualche modo, vantaggio – in termini di incremento di consumi – dallo sviluppo crescente di traffico di contenuti sulle proprie reti), ma è

1 *Ci si riferisce, nello specifico, all'attività di monitoraggio e mediazione svoltasi, sotto l'egida dell'AGCom, tra gli operatori coinvolti in relazione alla gestione dell'incremento del traffico sulle reti degli ISP derivante dalla fruizione (superiore rispetto a quanto accaduto in passato) degli incontri del Campionato di calcio di Serie A ed altri eventi sportivi, con la definizione delle modalità di messa in dotazione dei singoli ISP delle soluzioni tecniche atte a consentire tale circostanza e con soddisfazione finale di tutti i soggetti interessati.*

del tutto evidente che se l'interesse è quello di trovare una maniera di declinare tale questione, occorrerà superare l'attuale "muro contro muro" e provare ad individuare delle soluzioni di compromesso che possano soddisfare entrambi gli schieramenti.

QUALE TUTELA PER L'OPERA GENERATA DALL'A.I.?
IL NOSTRO DIRITTO D'AUTORE È TROPPO "ANTROPOMORFO"?

Andrea Amidei, Studio Legale Ruffolo

I sistemi di intelligenza artificiale (A.I.), o quantomeno taluni di essi, sono in grado di "creare" e "inventare", realizzando "opere dell'ingegno" o "invenzioni" quali risultati di attività posta in essere dalla macchina in modo più o meno indipendente dal controllo, contributo e intervento umano: da componimenti letterari o musicali a dipinti, sino a ritrovati che consentono soluzioni originali a problemi tecnici, suscettibili di applicazione industriale.

Se si confina l'analisi nel solo campo "artistico", escludendo dunque l'ambito della creazione di trovati di natura tecnica (nel quale pure l'A.I. ha dato ottima prova; si pensi al noto "caso DABUS"), osserviamo come il settore della creatività computazionale si estenda dalle applicazioni più semplici a quelle più complesse, dai traduttori agli applicativi utilizzati da redazioni giornalistiche per la predisposizione di articoli di cronaca o rassegne stampa. Ma si pensi anche al romanzo "The day a computer writes a novel", "scritto" nel 2015 in Giappone da un sistema di A.I. e risultato finalista in un premio letterario; o ancora al sistema "The New Rembrandt" di Microsoft, in grado di apprendere lo stile del pittore olandese e di riprodurlo per creare (non mere copie, ma) dipinti del tutto nuovi; o al disco musicale "Hello World", "inciso" da un'A.I. all'esito dell'elaborazione di innumerevoli dati di input consistenti nella traduzione in linguaggio machine-readable di ritmi, melodie e armonie.

L'interesse verso il tema trova oggi nuova linfa a fronte della diffusione di sistemi di A.I. basati su algoritmi generativi – quali i noti ChatGPT di OpenAI o Bard di Google – che, su specifica interrogazione (prompt) dell'utente, risultano capaci di creare testi anche

nuovi e "originali" quale esito dell'apprendimento derivante dalla elaborazione di dati e contenuti in rete. E sempre più ampia è la diffusione di sistemi in grado di generare immagini "nuove" sulla base di input costituiti da parole o frasi immesse dall'utilizzatore.

L'ingresso dell'A.I. nell'attività creativa ha suscitato un acceso dibattito tra chi si domanda se, e con quali strumenti, possa riconoscersi tutela alle opere generate dalla macchina, soprattutto in termini di copyright. In tema di diritto d'autore (ma analoghe questioni si pongono, mutatis mutandis, anche in materia brevettuale), ci si interroga, in particolare, sulla proteggibilità o meno di un'opera che, benché oggettivamente nuova e originale, possa, in quanto generata autonomamente dall'A.I. in assenza di apporto

«L'ingresso dell'A.I. nell'attività creativa ha suscitato un acceso dibattito tra chi si domanda se, e con quali strumenti, possa riconoscersi tutela alle opere generate dalla macchina, soprattutto in termini di copyright.»

(o con apporto molto limitato) dell'uomo, risultare carente di quel "fattore umano" che, secondo la tradizionale interpretazione delle norme in materia, deve connotare l'elemento della "creatività" (che costituisce, come è noto, requisito indispensabile ai fini del diritto d'autore).

Non occorre certo ricordare qui come l'attributo che più di ogni altro consente di differenziare l'A.I. da tecnologie software tradizionali risieda nella capacità di autonomia, nonché di autoapprendimento. La qual cosa, secondo i tecnici di settore, spesso determina, per le A.I. più evolute, un anche elevato livello di "opacità" del sistema, intesa come oggettiva impossibilità per l'essere umano – ivi incluso il programmatore, produttore o utilizzatore del sistema stesso – di prevedere, controllare e comprendere ex post non soltanto l'output dell'elaborazione della macchina, ma anche i meccanismi che vi hanno condotto. Ed è in tali peculiarità che a detta di molti si rinviene la principale difficoltà nel garantire tutela autoriale a un'opera generata dalla macchina a valle di un processo connotato da un livello di autonomia tale da ridurre anche ai minimi termini il contributo umano all'atto creativo.

Per vero, la fenomenologia dei sistemi di A.I. non appare omogenea quanto a capacità

di autonomia (e a opacità). Su tale assunto si fonda la comune distinzione tra opere A.I.-assisted e A.I.-generated: per le prime l'A.I. rileverebbe quale mero strumento di ausilio a un'attività creativa che resta in capo all'essere umano, e sotto il suo controllo, conseguendone la possibilità di applicare i tradizionali paradigmi della tutela autoriale; mentre nel secondo – più problematico – caso l'A.I. "creerebbe" in modo del tutto indipendente rispetto all'uomo, giungendo a risultati da quest'ultimo non prevedibili né condizionabili o governabili. Tracciare il discrimine tra le due tipologie di opere può rivelarsi, nei fatti, non sempre agevole, così come complesso risulta l'interrogativo su quale livello, e quale tipo, di intervento umano possa ritenersi necessario e sufficiente perché l'atto creativo non risulti imputabile esclusivamente alla "macchina".

Per le opere create dall'A.I. resta centrale, dunque, l'interpretazione del requisito della "creatività" dell'opera, tradizionalmente letto, anche con riferimento agli artt. 2576 c.c. e 6 l.d.a., come espressione e riflesso del lavoro intellettuale dell'uomo, e dunque della sua "individualità"; desumendosene, pur in assenza di espresse norme in tal senso, che "autore" di un'opera idonea ad ambire alla protezione autoriale possa essere soltanto un umano. Ne emerge una impostazione (forse troppo) antropocentrica – per non dire "antropomorfica" – del diritto d'autore, che pare talora contrastare, tra l'altro, con la dimensione di mercato progressivamente assunta dall'industria creativa, e con la crescente rilevanza acquisita – più che dai diritti morali – dalla sfera dei diritti patrimoniali sull'opera dell'ingegno e dei diritti connessi, oltre a rischiare di risultare fonte di seri disincentivi allo sviluppo tecnologico.

La tematica è complessa e queste brevi note non possono certo ospitarne una esaustiva trattazione. Basti allora chiarire, quantomeno a livello metodologico, che ad avviso di chi scrive – ove si ritengano inaccettabile la negazione di ogni tutela autoriale a tutte le opere dell'ingegno "create" dall'A.I. – le percorribili soluzioni, in assenza (e in attesa) di sviluppi normativi, dovrebbero prendere le mosse da una distinzione tra tutelabilità "oggettiva" dell'opera e attribuzione "soggettiva" dei relativi diritti (morali e patrimoniali). Trattasi, infatti, di due piani che, pur intersecandosi, non vengono necessariamente a coincidere, e la cui confusione potrebbe condurre a esiti non soltanto indesiderati, ma anche contrari alla ratio della normativa. Da un canto, allora, occorre preliminarmente domandarsi se l'opera A.I.-generated, in sé considerata quale "oggetto", possa presentare i requisiti necessari per il riconoscimento di tutela, e, poi, in caso di risposta positiva, interrogarsi

su chi debba essere il titolare dei diritti (soprattutto patrimoniali) su di essa.

Quanto al primo quesito, si dovrà riflettere su una nuova concezione di "creatività", nella consapevolezza di come essa possa non essere, con l'evolvere delle tecnologie, prerogativa necessariamente solo umana, risultando suscettibile di trovare declinazioni anche diverse: ci troviamo forse dinanzi a una forma di "creatività" diversa da quella umana – come diversa è l'"intelligenza" umana da quella artificiale – ma i cui effetti risultano forse non meno rilevanti per il diritto. E soluzione sia congrua che in linea con le vigenti norme potrebbe allora derivare non soltanto da una lettura evolutiva del requisito della "creatività", ma anche da una valorizzazione del ruolo umano nell'atto creativo, indagando su quale apporto dell'autore umano sia necessario e sufficiente a

«Quanto al primo quesito, si dovrà riflettere su una nuova concezione di "creatività", nella consapevolezza di come essa possa non essere, con l'evolvere delle tecnologie, prerogativa necessariamente solo umana, risultando suscettibile di trovare declinazioni anche diverse: ci troviamo forse dinanzi a una forma di "creatività" diversa da quella umana – come diversa è l'"intelligenza" umana da quella artificiale – ma i cui effetti risultano forse non meno rilevanti per il diritto.»

garantire tutela.

Un primo passo in tal senso sembra essere stato mosso dalla Corte di Cassazione, con un'ordinanza del gennaio 2023 (n. 1107/2023). Ordinanza che gli "entusiasmi della prima ora" hanno condotto i più a definire come la prima pronuncia italiana in materia di copyright su opere A.I.-generated, nonostante, per vero, la decisione concernesse un caso di opera generata non da un sistema di A.I., bensì da (o con l'ausilio di) un software "tradizionale". Ciononondimeno, nel vagliare il caso la Cassazione ha espresso principi suscettibili di contribuire al dibattito sul tema della protezione (anche) delle opere A.I.-generated, specialmente con riguardo all'interpretazione del requisito della "creatività".

In primo luogo, la Corte ha chiarito come il fatto di avere utilizzato un software per generare l'opera non sia di per sé sufficiente a escluderne la tutelabilità, ove ne ricorrano

i presupposti. Né, del resto, si aggiunge, la sussistenza di carattere creativo dell'opera è esclusa dal fatto che per addivenire alla sua realizzazione si pongano in essere attività di rielaborazione, manipolazione o rilettura, anche automatizzata, di elementi preesistenti, come tipico dell'A.I. generativa (fermi restando, ovviamente, come per le opere interamente "umane", il divieto di plagio di lavori altrui o di loro illecita apprensione).

Quanto all'individuazione, in termini sia qualitativi che quantitativi, dell'apporto umano nella realizzazione dell'opera, la Cassazione ha precisato, da un lato, che la verifica della sussistenza del requisito della "creatività" per opere computer-generated deve essere condotta con rigore maggiore rispetto a quello riservato a opere "tradizionali", valutando se l'utilizzo dello strumento informatico abbia o meno assorbito in toto l'elaborazione creativa di chi se ne avvalga; dall'altro, che l'apporto creativo umano può anche risultare "minimo", purché si rifletta nell'opera come risultato finale. E, al riguardo, la Corte UE ha più volte affermato che l'apporto creativo può riguardare anche una sola fase dell'elaborazione dell'opera, ove idoneo a testimoniare la scelta personale dell'autore; e dunque, potenzialmente, anche la fase di selezione degli input e dei task da assegnare al sistema autonomo, così come la fase di selezione, con eventuali modifiche, degli output da quest'ultimo prodotti.

LA CYBERSECURITY DELL'IA: TRA STANDARD E REGOLAZIONE

Daniele Amitrano, Trevisan & Cuonzo

Se è vero che i sistemi di IA sono sistemi informatici e, in quanto tali, ereditano tutti i rischi di cybersecurity già connessi ai sistemi digitali tradizionali che operano in contesti simili, è anche vero che il continuo sviluppo di sistemi di IA sempre più complessi sta generando nuovi rischi legati all'emergere di nuove classi di vulnerabilità specifiche.

Come noto, le istituzioni europee sono all'opera per finalizzare il Regolamento sull'Intelligenza Artificiale ("AI Act"), che affronta tra gli altri anche il tema della cybersecurity legata ai sistemi di IA definiti "ad alto rischio".

In particolare, l'art. 15 dell'AI Act prevede nuovi specifici obblighi di compliance per i produttori di sistemi IA ad alto rischio, richiedendo, da un lato, che tali sistemi siano progettati e sviluppati in modo tale da conseguire un livello adeguato di accuratezza, robustezza e cybersecurity e, dall'altro lato, che le soluzioni tecniche volte a garantire la cybersecurity di tali sistemi debbano essere adeguate alle circostanze e ai rischi pertinenti.

Come è stato di recente sottolineato dalla Commissione Europea nel proprio report sulla "Cybersecurity of Artificial Intelligence in the AI Act", pubblicato a settembre 2023, l'art. 15 dell'AI Act, ed in generale l'intera proposta di Regolamento, si applica ai sistemi di IA, secondo la definizione contenuta all'art. 3 dell'AI Act, e non invece ai singoli modelli di IA che compongono il sistema.

Si tratta di una precisazione importante, in quanto potrebbe accadere che siano immessi sul mercato sistemi di IA che combinano diversi modelli di IA, oltre a componenti

integrati come interfacce e database (si pensi, ad esempio, ad un chatbot che si basi, oltre che su Large Language Models, anche su una infrastruttura cloud tradizionale e su altri componenti software in grado di pre-processare gli input ricevuti). In queste situazioni, un approccio che si concentri sui singoli modelli piuttosto che sulla loro interazione potrebbe lasciare spazio a potenziali bug che potrebbero essere sfruttati durante un attacco informatico.

Con il citato report di settembre 2023, la Commissione Europea ha delineato alcuni importanti principi guida in relazione ai requisiti di cybersecurity dei sistemi di IA ad alto rischio.

«In particolare, l'art. 15 dell'AI Act prevede nuovi specifici obblighi di compliance per i produttori di sistemi IA ad alto rischio, richiedendo, da un lato, che tali sistemi siano progettati e sviluppati in modo tale da conseguire un livello adeguato di accuratezza, robustezza e cybersecurity e, dall'altro lato, che le soluzioni tecniche volte a garantire la cybersecurity di tali sistemi debbano essere adeguate alle circostanze e ai rischi pertinenti.»

In primo luogo, la conformità all'art. 15 dell'AI Act richiede una attenta valutazione del rischio di cybersecurity, con riferimento sia all'intero sistema di IA, sia ai singoli componenti (anche non IA). La valutazione del rischio di cybersecurity deve essere condotta a due livelli: un livello normativo generale e un livello speciale in relazione agli specifici rischi del singolo sistema di IA. Potrà pertanto accadere che, sebbene l'uso di un determinato sistema di IA possa essere considerato ad alto rischio ai sensi dell'AI Act, tale sistema possa presentare in concreto rischi limitati di cybersecurity a causa del modo in cui è stato progettato e funziona.

In secondo luogo, la verifica della sicurezza dei sistemi di IA richiede un approccio olistico integrato e continuo, durante l'intero ciclo di vita del sistema, che utilizzi pratiche collaudate e controlli specifici per il singolo sistema di IA. Si tratta di un principio fondamentale per i sistemi di IA, che imparano continuamente dal loro utilizzo e possono quindi generare bug e punti deboli potenzialmente sfruttabili dagli attori delle minacce informatiche che monitorano costantemente tali sistemi.

Una questione importante riguarda inoltre la standardizzazione come strumento di controllo della cybersecurity nei sistemi di IA.

A marzo 2023 la European Union Agency for Cybersecurity (ENISA) ha pubblicato un report[1] sulla "Cybersecurity of AI and standardisation" che analizza gli standard esistenti e in fase di studio relativi alla cybersecurity nei sistemi di IA e identifica alcune lacune nella standardizzazione.

«Lo stato dell'arte della sicurezza dei modelli di IA presenta infatti alcuni limiti. Data la molteplicità e la diversa maturità delle attuali tecnologie di IA, è indispensabile riconoscere che non tutte le tecnologie sono adatte ad essere impiegate in uno scenario ad alto rischio, salvo affrontare le loro carenze in termini di cybersecurity.»

Lo stato dell'arte della sicurezza dei modelli di IA presenta infatti alcuni limiti. Data la molteplicità e la diversa maturità delle attuali tecnologie di IA, è indispensabile riconoscere che non tutte le tecnologie sono adatte ad essere impiegate in uno scenario ad alto rischio, salvo affrontare le loro carenze in termini di cybersecurity.

La conformità ai requisiti di cybersecurity può essere raggiunta attraverso l'adozione degli standard armonizzati sviluppati dalle Standards-Developing Organisations (SDOs). A questo proposito, gli standard tecnici e organizzativi generali esistenti, come quelli della serie ISO/IEC 27000, possono mitigare i rischi informatici legati all'IA con indicazioni specifiche sulla loro applicazione in un contesto di IA.

Come osservato dall'ENISA, tuttavia, questo approccio potrebbe non essere esaustivo e presentare dei limiti.

Ad esempio, gli standard potrebbero non essere in grado di coprire approcci che vadano oltre l'attuale stato dell'arte in materia di IA, e quindi per alcuni sistemi emergenti di IA ad alto rischio potrebbe non essere possibile, seguendo tali standard, raggiungere

---

1 https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

la conformità con i requisiti di cybersecurity previsti dall'AI Act. Inoltre, gli standard che si focalizzano sul concetto tradizionale di software potrebbero trovare ostacoli alla loro applicazione ad un sistema di IA, che può comprendere anche elementi tecnici e organizzativi che vanno oltre il software, come l'hardware o l'infrastruttura. Infine, gli standard esistenti potrebbero non affrontare aspetti specifici come la tracciabilità dei flussi di dati e dei componenti IA o le metriche di robustezza.

Questi limiti non impediscono tuttavia necessariamente la conformità dei sistemi di IA che fanno uso di tecnologie emergenti ai requisiti di cybersecurity previsti dall'AI Act, né dovrebbero ostacolare lo sviluppo di standard. I sistemi di IA ad alto rischio possono comunque raggiungere la conformità se mitigano adeguatamente i rischi complessivi di cybersecurity del sistema attraverso altre misure complementari, seguendo un approccio integrato che combina pratiche e procedure di cybersecurity consolidate con misure specifiche per il singolo sistema di IA.

In questo quadro, è importante e auspicabile che il processo di standardizzazione si accompagni parallelamente a un progresso tecnologico negli strumenti di cybersecurity in grado di far fronte ai nuovi rischi emergenti.

UNA PROSPETTIVA SU SOFTWARE SECURITY E VULNERABILITY MANAGEMENT

Davide Ariu, Pluribus One

Quello della sicurezza del software è oggigiorno uno dei fronti più caldi della cybersecurity, per almeno due ragioni.

Da una parte c'è una spinta normativa verso l'adozione di pratiche e procedure da parte di chi immette a qualche titolo componenti software sul mercato a fare in modo che questo software sia il più possibile sicuro ed esente da vulnerabilità.

Sulla sponda orientale dell'Atlantico la Commissione Europea si appresta infatti a varare il Cyber Resilience Act, che ha ne "la riduzione del numero di vulnerabilità nei prodotti hardware e software" uno dei suoi due obiettivi chiave. Sulla sponda occidentale, già nel 2021 un ordine esecutivo del presidente degli Stati Uniti, finalizzato ad incrementare la sicurezza cyber del paese, prevedeva un insieme di interventi finalizzati ad incrementare la sicurezza delle software supply-chain in relazione ai software in uso da parte del governo americano.

Dall'altra parte abbiamo un dato oggettivo. Il crescente numero di attacchi alimenta la corsa alla riduzione del rischio di cui nell'ambito della quale il tema della gestione delle vulnerabilità è evidentemente centrale.

Cercheremo nelle righe che seguono di guardare dunque ai processi di Vulnerability Management più da vicino, scattando una fotografia di alcuni dei trend chiave ad esso connessi.

FIRST[1], associazione internazionale di first responders, intende con servizi di Vulnerability Management quelli relativi alla scoperta, analisi e gestione di vulnerabilità nuove o riportate all'interno dei sistemi informativi. Il dato rilevante, in relazione alle vulnerabilità pubblicamente riportate, è che il loro numero è in costante e significativo aumento da anni. Il 2023 si chiuderà con un incremento rispetto al 2022 compreso fra il 15 e il 20%, mentre negli ultimi 5 anni il numero di vulnerabilità è praticamente raddoppiato. Perché questo dato è preoccupante? Principalmente perché deve essere valutato in relazione ad una cronica incapacità delle aziende di tenere il passo, con i processi di vulnerability management e patching, rispetto al numero di vulnerabilità pubblicate. Uno studio interessante di Kenna Security (ora CISCO) e del Cyentia Institute[2] dice che la quantità di vulnerabilità che un'organizzazione può correggere è nell'ordine del 10-15% di quelle scoperte. Visto da un'altra prospettiva, ciò significa che c'è l'85-90% di vulnerabilità che viene accumulato in un backlog e che probabilmente rimarrà lì per molto tempo.

«Il dato rilevante, in relazione alle vulnerabilità pubblicamente riportate, è che il loro numero è in costante e significativo aumento da anni. Il 2023 si chiuderà con un incremento rispetto al 2022 compreso fra il 15 e il 20%, mentre negli ultimi 5 anni il numero di vulnerabilità è praticamente raddoppiato.»

Ma cosa succede a queste vulnerabilità non gestite? Se un sistema è presente una vulnerabilità da questa discende un potenziale rischio, legato proprio alla possibilità di un attacco che sfrutti quella vulnerabilità.

Va comunque precisato che non di tutte le vulnerabilità viene realizzato un exploit, ovvero un codice software che consenta di sfruttarla. Affinché una vulnerabilità sia

1 *FIRST.org – FIRST è un'associazione di rilievo internazionale che raggruppa i Cyber Security Incident Response Teams. È responsabile per lo sviluppo dei due principali sistemi di scoring delle vulnerabilità, gli standard CVSS e EPSS.*

2 *Rapporto fra il numero di vulnerabilità osservate e gestite. Source: Prioritization To Prediction (Vol. 8), CISCO/CYENTIA INSTITUTE.*

appetibile per lo sfruttamento su larga scala devono essere infatti soddisfatte almeno tre condizioni:

1. Il "pubblico" (inteso come numero di soluzioni e sistemi) affetto dalla vulnerabilità deve essere vasto, cosicché lo sforzo di sviluppo dell'exploit possa essere sostenuto a fronte di una congrua prospettiva di ritorno;

2. La vulnerabilità deve poter essere sfruttata "agevolmente": l'operazione di attacco deve poter essere eseguita su larga scala con sistemi automatici;

3. Lo sfruttamento della vulnerabilità deve avere un impatto significativo, ovvero deve consentire accesso a dati riservati o acquisire il controllo della macchina o dei sistemi che ne sono affetti.

Se questi requisiti sono soddisfatti, mediamente chi attacca impiega circa venti giorni (secondo uno studio Qualys) per la cosiddetta "weaponization", ovvero per sfruttare la vulnerabilità attraverso la predisposizione di un exploit da inserire magari all'interno di una suite di attacco automatico[3]. Lo stesso studio ci dice che i tempi necessari alla correzione della vulnerabilità (per quelle vulnerabilità che vengono effettivamente corrette) da parte di chi si difende sono di trenta giorni, con una finestra di vulnerabilità media di circa dieci giorni.

Come anticipato sopra però non tutte le vulnerabilità vengono effettivamente sfruttate, e c'è in questo una buona notizia, che possiamo cogliere se andiamo a valutare la percentuale di vulnerabilità per cui esiste effettivamente un exploit pubblico e di cui abbiamo evidenza pubblica del fatto che stiano venendo sfruttate. Tale percentuale[4] è nell'ordine del 5%, che significa che è questo il sottoinsieme di vulnerabilità di cui dovremmo effettivamente preoccuparci. Per l'80% delle vulnerabilità non esiste infatti un exploit mentre il 66% di vulnerabilità non è identificabile automaticamente tramite uno strumento di scansione lanciato contro i sistemi affetti, requisito essenziale ai fini dello sfruttamento automatico su larga scala e di un agevole e sostanziale ritorno (economico) per chi attacca.

---

3 Uno strumento frequentemente utilizzato a questo scopo è Metasploit – https://www.metasploit.com.

4 Distribution of vulnerabilities between Observed-Not Observed and Exploited – Not Exploited. Source: Prioritization To Prediction (Vol. 5), CISCO/CYENTIA INSTITUTE

Dunque, a fronte di un aumento molto importante del numero di vulnerabilità, esiste la possibilità di concentrarsi su un numero più limitato di vulnerabilità rispetto a quelle pubblicate, che sono quelle che hanno il potenziale di essere realmente sfruttate.

Per favorire questo processo sono state lanciate nel corso degli ultimi anni alcune iniziative interessanti che vanno oltre la storica misura di gravità tecnica (lo score CVSS[5]) e consentono di agevolare il lavoro di prioritizzazione. Una è l'Exploit Prediction Scoring System (EPSS[6]), ovvero un meccanismo di scoring delle vulnerabilità che attribuisce a ciascuna vulnerabilità un punteggio da 0 a 1 indicativo della probabilità che questa venga realmente sfruttata. Le vulnerabilità con punteggio EPSS prossimo al valore "1" sono quelle alle quali deve essere attribuita massima priorità nel processo di mitigazione. L'indicatore viene aggiornato da FIRST su base giornaliera e tiene conto di molteplici fattori compresi, fra gli altri, la presenza di un exploit pubblico, il vendor affetto dalla vulnerabilità, e attività di monitoraggio dei social e piattaforme pubbliche.

«Dunque, a fronte di un aumento molto importante del numero di vulnerabilità, esiste la possibilità di concentrarsi su un numero più limitato di vulnerabilità rispetto a quelle pubblicate, che sono quelle che hanno il potenziale di essere realmente sfruttate.»

La seconda è un'iniziativa della Cybersecurity & Infrastructure Security Agency del governo statunitense, che aggiorna quotidianamente il Known Exploited Vulnerabilities Catalog. Si tratta, in questo caso, del "catalogo" delle vulnerabilità delle quali esiste evidenza di sfruttamento all'interno dei sistemi degli enti pubblici americani, che evidentemente costituisce una buona base di partenza nello stilare una lista di priorità.

5 *CVSS – Common Vulnerability Scoring System - https://www.first.org/cvss/*

6 *EPSS - Exploit Prediction Scoring System - https://www.first.org/epss/*

DEEPFAKE E
AI GENERATIVE

Sebastiano Battiato, Università di Catania

“Seeing is Believing”, addio! Con l’avvento delle recenti tecnologie basate appunto sulla cosiddetta Intelligenza Artificiale Generativa, sarà sempre più complicato, per gli esseri umani per loro natura intrinsecamente “analogici”, riuscire a distinguere un contenuto multimediale “fake” da uno reale. Molteplici sono gli esempi che si susseguono, oramai ad un ritmo frenetico, in cui vuoi per gioco, vuoi per profitto o per fama/vendetta, in contesti pubblici e/o privati, i Deepfake vengono utilizzati e diffusi sui vari canali social e non solo. I nostri sistemi cognitivi non sono oramai in grado di cogliere alcuna differenza sostanziale “percettiva” ed infatti, rimaniamo stupiti nel ascoltare voci sintetiche, volti animati perfettamente integrati e indistinguibili dal presunto originale.

Recenti studi hanno inoltre dimostrato come il famoso “Test di Turing”, orientato a verificare se solo tramite chat fosse possibile decidere della presunta “umanità” dell'interlocutore, sia destinato a fallire nel breve termine. Il termine “Deep” sta a sottolineare la strategia computazionale utilizzata in ambito AI, per addestrare Reti Neurali Artificiali cosiddette “profonde”, cioè con un numero di parametri intrinseci particolarmente elevato, e soprattutto ideata con la capacità di analizzare ed “imparare” strutture, pattern e correlazioni nascoste negli altrettanto numerosi dati di ingresso, forniti come esempio. Potremmo citare a tal scopo, proprio per rimanere su temi di cronaca recente, “Now and Then” dei Beatles, oppure la foto di Papa Francesco con indosso il piumino bianco. Ma gli esempi sono destinati a crescere, a tal punto che qualcuno profetizza che le future camere digitali dei nostri smartphone potrebbero essere sostituite “grossolanamente” da appositi AI-tools che generano immagini/

video a comando. Senza dilungarsi sui dettagli tecnici che stanno alla base di tali "meraviglie", possiamo altresì sintetizzare il fatto che le moderne macchine basate sul cosiddetto Deep Learning generativo e, più di recente, grazie al supporto dei cosiddetti Foundational Models (stile Chat GPT per intendersi), sono in grado di analizzare quantità inimmaginabili di esempi e, mediante tecniche "adversariali" o pseudo tali, generare contenuti "credibili" con una qualità percettiva mai vista prima. Se a questo aggiungiamo la cosiddetta "democratizzazione della produzione audiovisiva", intendendo con ciò che i tools di sviluppo AI-based sono alla portata di tutti perché resi disponibili a basso costo, possiamo affermare che la certificazione della cosiddetta autenticità di un segnale multimediale diverrà sempre più attuale e complicata.

«Recenti studi hanno inoltre dimostrato come il famoso "Test di Turing", orientato a verificare se solo tramite chat fosse possibile decidere della presunta "umanità" dell'interlocutore, sia destinato a fallire nel breve termine.»

D'altra parte gli addetti ai lavori stanno già rilasciando opportuni adeguamenti alle best practice di settore, in cui in analogia a quanto fatto finora, si va alla ricerca con metodi tradizionali o con ulteriori tools basati sempre su AI, di tracce dell'"innaturalezza" dell'informazione rappresentata nel segnale da analizzare. Per quanto le macchine siano in grado di ingannare il nostro vetusto occhio biologico, non tutte le innumerevoli statistiche naturali sono riprodotte fedelmente, per cui il buon caro vecchio investigatore/tecnico forense ante-litteram è ancora necessario, utile e determinante nella risoluzione di diatribe sulla presunta autenticità di clip multimediali.

Il futuro ovviamente è da scrivere. Anche in questo caso però dobbiamo assolutamente ribadire come le scoperte scientifiche e la comunità accademica siano assolutamente da considerarsi come stabile approdo cui affidarsi per garantire l'utilizzo consapevole, trasparente e ove possibile sicuro e scevro da potenziali bias di sviluppo e/o dei dati utilizzati delle attuali e future macchine calcolatrici AI-based.

GIUSTIZIA PREDITTIVA

Manuel Caccone, LexCapital

GIUSTIZIA PREDITTIVA, IL CONTENZIOSO CIVILE COME OPERAZIONE FINANZIARIA ALEATORIA

Nel contesto specifico del finanziamento delle controversie e della giustizia predittiva, è cruciale comprendere che l'uso avanzato dell'analisi dei dati e delle previsioni basate su modelli di intelligenza artificiale non può essere ridotto a una semplice "truffa" o a un gioco d'azzardo. Questi strumenti avanzati offrono una visione amplificata e potenziata dalle probabilità, basata su dati empirici e analisi storiche. Tuttavia, non possono sostituire la saggezza, l'intuizione e la profonda comprensione del campo che solo un esperto può portare. La tecnologia rivoluzionaria di LexCapital sta sviluppando un nuovo capitolo nel campo emergente della giustizia predittiva, che mira a prevedere l'esito di una causa o di una sentenza. Questo non è un semplice speculazione, ma un approccio basato su dati, analisi e modelli storici. L'applicazione di questi strumenti è ampia e variegata, con magistrati e avvocati che li utilizzano per ottenere informazioni e proiezioni prima di pronunciare una sentenza. Tuttavia, è essenziale distinguere una distinzione cruciale: mentre la giustizia predittiva può aiutare a prevedere l'esito di una sentenza, essa non consente una decisione automatizzata tramite l'IA. La decisione finale dovrebbe sempre basarsi sull'esperienza e il giudizio umano. Il contenzioso civile può essere interpretato sotto una lente finanziaria come un'operazione aleatoria, in quanto si riferisce alla presenza di incertezza e variabilità negli esiti e nei costi. La parte che decide di intraprendere un'azione legale lo fa con la speranza di ottenere un rendimento (ad esempio, una sentenza favorevole o un risarcimento). L'esito non è certo e può variare a seconda delle circostanze.

LITIGATION FUNDING: UN'OPERAZIONE ALEATORIA CONTRATTUALMENTE ATIPICA

L'evoluzione dell'analisi predittiva nel campo legale ha aperto nuove porte e migliorato le capacità dei professionisti del diritto, ridefinendo il modo in cui vengono prese e interpretate le decisioni legali. I modelli di Elaborazione del Linguaggio Naturale (NLP) hanno rivoluzionato il modo in cui le informazioni legali vengono elaborate e analizzate. Il NLP può leggere e compilare grandi volumi di testi legali, identificando pattern e tendenze. Tuttavia, la sua capacità unica di distinguere tra sfumature linguistiche e interpretative lo rende particolarmente utile in questo contesto.

Il NLP ha portato all'emergere di piattaforme e software che integrano queste capacità analitiche, consentendo ricerche giurisprudenziali più rapide, analisi comparative delle decisioni e previsioni accurate basate sui dati. Questi sistemi migliorano anche il modo in cui gli avvocati interagiscono con i loro clienti, fornendo consigli più accurati e un migliore servizio clienti.

«L'evoluzione dell'analisi predittiva nel campo legale ha aperto nuove porte e migliorato le capacità dei professionisti del diritto, ridefinendo il modo in cui vengono prese e interpretate le decisioni legali. I modelli di Elaborazione del Linguaggio Naturale (NLP) hanno rivoluzionato il modo in cui le informazioni legali vengono elaborate e analizzate.»

L'INTELLIGENZA ARTIFICIALE: UN ALLEATO, NON UN SOSTITUTO

È essenziale ricordare che la tecnologia non sostituirà completamente il giudizio, l'esperienza e l'intuizione umana. Invece, l'IA può essere vista come un compagno nel viaggio degli esseri umani, aiutandoli a comprendere e prendere decisioni informate. Può fornire insights basati sull'analisi dei dati, ma è anche suscettibile di errori e pregiudizi. Pertanto, la supervisione continua, la convalida e il miglioramento delle soluzioni basate sull'IA sono cruciali per garantire che il loro utilizzo sia etico e responsabile.

ANALISI DEL TESTO GIURIDICO: DALL'INTERPRETAZIONE ALL'ASTRAZIONE GRAZIE ALL'IA

L'analisi della prova giudiziaria è sempre stata una sfida cruciale per i professionisti del diritto, compresi avvocati, giudici e magistrati. Tuttavia, l'avvento delle tecnologie dell'intelligenza artificiale sta rivoluzionando il processo. L'interpretazione tradizionale implica una combinazione di logica, esperienza, conoscenza della legge e comprensione del contesto sociale e politico. Gli algoritmi di apprendimento automatico hanno dimostrato notevoli capacità nell'interpretare il linguaggio naturale, identificando pattern, relazioni e situazioni complesse.

L'astrazione e la categorizzazione sono un'altra area in cui l'intelligenza artificiale eccelle, identificando principi generali in casi specifici. L'IA può anche aiutare a prevedere l'esecuzione di sentenze specifiche basate su precedenti e tendenze. La personalizzazione e la consulenza possono essere realizzate utilizzando l'IA per creare strumenti di consulenza personalizzati.

LA STANDARDIZZAZIONE DEL LINGUAGGIO GIURIDICO ATTRAVERSO IL NLP

L'introduzione dell'IA nell'analisi giudiziaria sta portando nuove possibilità e sfide. È essenziale mantenere un approccio critico e combinare le capacità della macchina con la profondità e l'umanità dell'interpretazione umana. I modelli di Elaborazione del Linguaggio Naturale (NLP) sono uno strumento fondamentale in questo contesto, aiutando a standardizzare il linguaggio legale e ridurre potenziali ambiguità.

ANALISI PREDITTIVA E ORIENTAMENTI GIURISPRUDENZIALI, DATI, PROBABILITÀ E DECISIONI INFORMATE

I modelli di Elaborazione del Linguaggio Naturale (NLP) hanno rivoluzionato il campo legale fornendo capacità avanzate per analizzare, interpretare e prevedere orientamenti giudiziari. Questi modelli possono identificare non solo tendenze manifeste, ma anche disposizioni e pattern ricorrenti che potrebbero non essere immediatamente evidenti per gli osservatori umani. Combinando informazioni dettagliate con approfondite intuizioni, questi modelli possono fornire previsioni accurate su come un tribunale potrebbe guidare e decidere in futuri casi con temi o contesti simili.

LA GIUSTIZIA PREDITTIVA: PREVEDERE L'INEFFICIENZA DEI TRIBUNALI ATTRAVERSO I DATI

La vasta quantità di dati giurisprudenziali fornisce una risorsa inestimabile per avvocati e altri professionisti del diritto. Con accesso all'analisi dei dati storici, gli avvocati possono ottenere una visione più chiara del panorama legale, consentendo loro di formulare strategie legali più efficaci e informate. La capacità di prevedere possibili esiti e orientamenti giudiziari può migliorare significativamente le possibilità di successo sia in aula che al di fuori del finanziamento delle controversie.

L'uso di modelli statistici avanzati e algoritmi sofisticati per effettuare previsioni legali è sempre più importante nel campo legale. È cruciale però comprendere che questi modelli non sono equivalenti a un tradizionale "azzardo" basato sull'intuizione o sul rischio. Sebbene un modello predittivo possa suggerire una probabilità elevata di successo in una causa legale, ci sono varie sfide da considerare.

«In conclusione, l'avvento della giustizia predittiva e degli strumenti avanzati di analisi dei dati rappresenta un significativo passo avanti per il settore legale. È essenziale però adottare un approccio equilibrato, in cui la tecnologia avanzi di pari passo con la saggezza e l'esperienza umana.»

La natura intrinseca della previsione comporta sempre un certo grado di incertezza, che può manifestarsi a causa di fattori come la qualità dell'input, l'accuratezza e la presenza di variabili sconosciute. Tuttavia, questi strumenti offrono una visione profonda e dettagliata delle probabilità, consentendo ai professionisti di prendere decisioni informate basate su dati empirici, metodi scientifici e precisione.

In conclusione, l'avvento della giustizia predittiva e degli strumenti avanzati di analisi dei dati rappresenta un significativo passo avanti per il settore legale. È essenziale però adottare un approccio equilibrato, in cui la tecnologia avanzi di pari passo con la saggezza e l'esperienza umana. Combinando questi elementi, si può raggiungere un sistema legale più efficiente, equo e preciso, in cui le decisioni sono informate dalla tecnologia ma guidate e modulate dall'esperienza umana.

L'INTELLIGENZA ARTIFICIALE NELL'ACCELERAZIONE DELL'ACQUISIZIONE DEI CONTENZIOSI: OPPORTUNITÀ E SFIDE

L'intelligenza artificiale ha trasformato vari settori, in particolare nell'acquisizione di contenuti da procedure concorsuali e difficoltà finanziarie temporanee. Ciò è dovuto alle opportunità offerte nella gestione dei pagamenti anticipati, parziali o totali, ai creditori.

Durante le crisi economiche, molte aziende affrontano difficoltà finanziarie temporanee o intraprendono procedure concorsuali, dando luogo all'emergere di contenuti che rappresentano una potenziale fonte di recupero finanziario per queste aziende. Una delle principali sfide per queste aziende è la liquidità. La possibilità di ricevere pagamenti anticipati per i contenuti in corso può rappresentare una preziosa risorsa finanziaria. L'IA offre un'analisi rapida e precisa di grandi quantità di dati legali, finanziari e operativi per valutare la probabilità di successo di un contenuto e il suo valore monetario. Consente ai potenziali acquirenti di contenuti di formulare offerte più informate e tempestive. L'IA può anche prevedere i rischi associati a determinati contenuti, garantendo termini di pagamento più equi e bilanciati.

LITIGATION FUNDING GUIDATO DALL'IA: PREVEDERE IL CHURN GIUDIZIARIO DEI RICORRENTI

L'IA sta cambiando il modo in cui avviene l'acquisizione di contenuti, offrendo nuove modalità alle aziende di migliorare la propria situazione. Tuttavia, è cruciale procedere con cautela e integrità, garantendo che le tecnologie siano utilizzate in modo efficiente e trasparente. Nel contesto legale, l'IA viene utilizzata per prevedere il "churn giudiziale" dei creditori. Ci riferiamo al fenomeno in cui un creditore decide di revocare o non procedere con una causa legale. Utilizzando algoritmi avanzati e dati storici, l'IA può identificare pattern che portano a un churn giudiziale, riducendo il rischio di perdite.

L'uso dell'IA per prevedere il churn giudiziale ha diversi vantaggi, tra cui un maggiore livello di trasparenza, una riduzione del rischio, una minor probabilità di perdite e un maggiore accesso alla giustizia. Con l'evoluzione dell'IA, essa continuerà a svolgere un ruolo significativo nel settore finanziario.

I TEMPI GIUDIZIARI COME DRIVER DI COSTO: MODELLARE LO SMONTAMENTO DI FLUSSI FINANZIARI CON PREVISIONI ACCURATE

In qualsiasi sistema legale, i giudici svolgono un ruolo cruciale nella determinazione dei costi associati alle procedure legali. Procedure giudiziarie lunghe e imprevedibili possono comportare notevoli svantaggi per le parti coinvolte, sia in termini di risorse finanziarie che di opportunità potenziali. Prevedere con precisione i tempi dei giudici è essenziale per modellare e gestire flussi finanziari dedicati alle procedure legali, e previsioni accurate sui tempi possono influenzare la gestione finanziaria.

«L'evoluzione tecnologica ha introdotto significative innovazioni nel campo della giustizia, tra cui l'analisi predittiva. Tuttavia, è essenziale che i professionisti adottino un approccio equilibrato, riconoscendo il potenziale di questi strumenti senza assumere la loro infallibilità.»

I lunghi periodi giudiziari non solo comportano ritardi nella risoluzione delle dispute, ma generano anche costi aggiuntivi, tra cui onorari legali, costi amministrativi, possibili danni alla reputazione e costi emotivi. Con l'avvento delle tecnologie avanzate e dell'analisi dei big data, è ora possibile effettuare previsioni più accurate sui tempi dei giudici. Ciò include la previsione della durata probabile di una procedura, la stabilizzazione di pattern ricorrenti nei ritardi giudiziari e l'identificazione di potenziali colli di bottiglia.

Previsioni accurate consentono alle organizzazioni e alle persone di allocare risorse, gestire il flusso di cassa e valutare alternative potenziali, come la mediazione o la transazione. Quando i tempi dei giudici non vengono analizzati e previsti con precisione, possono diventare un importante fattore di costo. Previsioni accurate sui tempi, alimentate da un'analisi avanzata dei dati, offrono l'opportunità di ridurre i rischi finanziari associati alle procedure legali.

LE FASI INTERMEDIE DEL GIUDIZIO: MODELING DEI TEMPI E DELLE MODALITÀ DI TRANSAZIONE

Il sistema giudiziario è complesso, con le sue intricate fasi e procedure. Le fasi intermedie del processo giudiziario svolgono un ruolo cruciale nella determinazione dell'esito di una controversia. Altri aspetti importanti includono il tempo di conclusione e la modalità di transazione. Questi elementi possono influenzare significativamente la "commissione di successo" del sistema legale, ovvero le commissioni percepite in base all'esito. La "modellazione" del tempo può essere ottenuta attraverso l'analisi rigorosa e l'uso della tecnologia, come algoritmi e intelligenza artificiale. La transazione, una negoziazione tra le parti per risolvere una controversia senza giungere a una sentenza finale, può ridurre significativamente il tempo della procedura. Questo modello può incentivare gli avvocati a lavorare in modo efficiente e professionale nelle fasi intermedie e a optare per la transazione quando è nell'interesse del cliente, garantendo un esito favorevole in tempi più brevi. La modellazione accurata del tempo e delle modalità di transazione può anche fornire informazioni legali su come ottimizzare le strategie, aumentando le commissioni di successo.

CONCLUSIONI

L'evoluzione tecnologica ha introdotto significative innovazioni nel campo della giustizia, tra cui l'analisi predittiva. Tuttavia, è essenziale che i professionisti adottino un approccio equilibrato, riconoscendo il potenziale di questi strumenti senza assumere la loro infallibilità. La giustizia predittiva offre una risorsa importante per navigare scenari legali complessi, ma è fondamentale affrontare questo meccanismo con trasparenza e integrità, garantendo che le decisioni finanziarie siano basate sugli interessi della giustizia piuttosto che sui profitti economici.

GIUDICI, HACKER E GIORNALISTI: LA CORSA ALL'ORO DELLA DIGITAL FORENSICS E PERCHÉ DOVREMMO CAMBIARE GIOCO

Alessandro Cantelli Forti, CNIT

Apprezzo lo spazio concesso in questa pubblicazione, un'opportunità per approfondire argomenti che, a causa di sopraggiunte restrizioni di tempo nella conferenza Legal Tech Forum 2023, sono rimasti solo introdotti.

In Italia, il rapporto tra avvocati e popolazione è tra i più alti nell'Unione Europea, con circa quattro avvocati ogni mille abitanti. Questa densità di professionisti legali si trova a confrontarsi con un'era in cui i sistemi digitali permeano ogni aspetto della vita, sia privata che professionale. Conseguentemente, una porzione sempre più significativa delle prove in ambito legale deriva da fonti digitali. Si tratta di elementi come scatole nere, sistemi di sorveglianza, dispositivi mobili, computer, database, server e sistemi industriali. Questa evoluzione ha dato vita a un mercato in rapida espansione per i "consulenti tecnici" del digitale, esperti specializzati nel campo della Digital Forensics. Le loro competenze sono sempre più richieste da istituzioni, aziende e privati, tanto che il valore di questo mercato era stato stimato in circa 50 milioni di euro nel 2018, che dovrebbe raggiungere i 100 milioni nel 2023. In risposta a questa crescente domanda, aziende leader nel settore della consulenza come Accenture, PwC e McKinsey stanno investendo in laboratori avanzati di Digital Forensics.

I consulenti tecnici operano in diversi contesti: al servizio dei Giudici, dove sono noti come periti o consulenti tecnici d'ufficio (C.T.U.), oppure a supporto di procure e delle parti in causa, in qualità di consulenti tecnici di parte (C.T.P.).

In ambito penale si presti molta attenzione ad usare il termine "Perito" e non "Consulente

Tecnico d'ufficio"! Ci tengo a ricordarlo in quanto le mie esperienze più grottesche in ambito Legal Tech derivano da collaborazioni con professionisti che, sempre con un senso di offesa quasi teatrale, schivano questioni sostanziali per trascinarti in questa lezione di campo semantico tra termini. Comunque, tra addetti ai lavori, si parla di C.T.U, C.T.P anche nell'ambito penale e di C.T.PM quando il consulente di parte è ingaggiato dal procuratore.

Attualmente, nonostante l'esigenza di una specializzazione marcata dovuta alla differenza sistemica tra periti e C.T.P., non esiste una "separazione delle carriere". Questa differenziazione sarebbe analoga a quella esistente tra giudici e avvocati. Penso che una distinzione chiara sarebbe necessaria non solo per evitare potenziali conflitti di interesse e questioni di opportunità, ma anche per riconoscere le diverse mentalità, competenze tecniche e conoscenze procedurali richieste dai due ruoli.

«In Italia, il rapporto tra avvocati e popolazione è tra i più alti nell'Unione Europea, con circa quattro avvocati ogni mille abitanti. Questa densità di professionisti legali si trova a confrontarsi con un'era in cui i sistemi digitali permeano ogni aspetto della vita, sia privata che professionale. Conseguentemente, una porzione sempre più significativa delle prove in ambito legale deriva da fonti digitali.»

Parlando ancora di periti e consulenti vari, esiste in Italia un numero crescente di professionisti del Legal Tech come lavoro a tempo pieno (e vera e propria passione).

Oltre ai cosiddetti professionisti, è utile menzionare anche i ricercatori, professori e personale accademico che hanno servito tribunali e procure per tutti i disastri di rilevanza nazionale, indagando incidenti ad ogni tipo di infrastruttura critica di trasporto come navi, treni, aerei ed impianti a fune. Per fare qualche esempio, persone che sono impiegate nel mondo accademico e della ricerca hanno lavorato ai casi di Ustica, Cermis, Moby Prince, Costa Concordia, torre piloti di Genova, Norman Atlantic fino ai casi più recenti o attualmente ancora in attesa di passare in giudicato.

Nei più recenti disastri analizzati è stata riscontrata una sovrapposizione dell'errore umano e del problema di natura tecnica. La relazione può avvenire in entrambi i sensi: o l'errore umano non viene completamente mitigato dal meccanismo di sicurezza preposto oppure un guasto tecnico non viene tempestivamente gestito dal personale. Questa interazione bidirezionale tra uomo e tecnologia è spesso il punto critico che porta al disastro.

Quello che dovrebbe accomunare le indagini sui disastri è la necessità di un approccio che sia non solo professionale, ma prevalentemente accademico, o meglio di ricerca, per espletare l'incarico. Questo è necessario perché molte informazioni di natura digitale devono essere elaborate tramite strumenti software, e talvolta hardware, creati ex novo in assenza di strumenti commerciali specifici.

Altri elementi che differenziano le indagini sui disastri sono la mancanza di precedenti, di documentazione tecnica completa e di strumenti automatici e già collaudati. Sfidanti sono infatti sia la quantità che la qualità eterogenea dei dati digitali da correlare.

L'impiego di personale accademico consente inoltre di analizzare il caso attraverso l'occhio di esperti "fuori da circoli ristretti". Tutti gli scenari menzionati nel mondo dei trasporti (e non solo) ruotano attorno a un numero davvero esiguo di persone, che si conoscono tutte. Si presume, e si spera, che il personale accademico possa acquisire una conoscenza specifica per ciascun caso senza essere pregiudizialmente influenzati da abitudini, preconcetti o legami professionali preesistenti. Inoltre, la forma mentis non solo deve rimanere aperta e neutrale nei confronti degli attori del processo, ma anche essere critica verso le stesse normative, internazionali e ministeriali, alla base dei diversi casi affrontati. Questo tipo di indagini dura anni e richiede molto studio e preparazione; quindi, difficilmente risulta appetibile da parte di un professionista affermato che potrebbe non ammortizzare i costi.

L'approccio accademico assume un valore particolarmente significativo in Italia, dove l'indagine penale tende ad avere la precedenza rispetto alle indagini tecniche condotte dai ministeri. Queste ultime sono principalmente volte a mitigare futuri incidenti piuttosto che a individuare le responsabilità. Inoltre, gli organismi dei vari uffici ministeriali non sempre dispongono del personale e degli strumenti necessari per gestire attività particolarmente complesse, pertanto si affidano a liste di "esperti", ovvero consulenti esterni.

Dalla mia esperienza personale, ho notato che gli organi investigativi ministeriali non hanno sempre accesso completo ai fascicoli dei giudici e non sono sempre coinvolti in tutte le fasi tecniche del contraddittorio. In aggiunta, i consulenti ministeriali devono spesso fornire risultati rapidamente alle controparti internazionali, il che può compromettere la completezza dell'analisi. Per questi motivi, l'indagine penale si rivela centrale anche per la sicurezza in un senso più ampio. Questa richiede dedizione, apertura mentale, competenza e soprattutto tempo, risorse che non sono sempre disponibili per un professionista, specialmente se sottopagato.

«Nei più recenti disastri analizzati è stata riscontrata una sovrapposizione dell'errore umano e del problema di natura tecnica. La relazione può avvenire in entrambi i sensi: o l'errore umano non viene completamente mitigato dal meccanismo di sicurezza preposto oppure un guasto tecnico non viene tempestivamente gestito dal personale. Questa interazione bidirezionale tra uomo e tecnologia è spesso il punto critico che porta al disastro.»

D'altro canto, collaborando da vicino con i più noti consulenti "professionisti" italiani, si percepisce un potenziale limite nella cultura nazionale della sicurezza, un elemento di criticità che, abbiamo detto, passa dall'indagine penale.

È ovvio che la maggior parte degli incarichi riguarda l'analisi di fonti digitali come cellulari, computer personali e telecamere di sorveglianza. Spesso, la quantità di dati da queste fonti è soverchiante, rendendo necessario personale extra e l'uso di strumenti commerciali per l'estrazione e l'analisi, gestiti da un tecnico specificamente formato, quindi non accademico, ma costantemente aggiornato ed allenato in questi dispositivi.

Questi strumenti, oltre a celare il loro funzionamento interno e a non essere certificati da nessun organismo ufficiale, tranne rari casi, sono estremamente costosi (decine di migliaia di euro per anno) e costringono i consulenti tecnici a lavorare in modo intensivo, a volte giorno e notte, per ammortizzare il costo. Considerando che i tribunali o le procure pagano tra i 4 e gli 8 euro all'ora, con saldi posticipati di oltre un anno,

chi investe in laboratori e nelle licenze di questi software deve necessariamente accettare anche incarichi privati, remunerati centinaia di euro all'ora. Di conseguenza, molti "professionisti" accettano incarichi d'ufficio principalmente come vetrina e per costruire rapporti di fiducia con i giudici, potenzialmente spendibili in future consulenze private. Questa dinamica "vetrina" si estende anche al mondo dei media: la notorietà in casi di alto profilo ha trasformato alcuni consulenti in volti noti della TV, ospiti fissi di talk-show sul crimine.

Posso garantire che alcuni consulenti molto affermati accettano incarichi pubblici, e quindi sottopagati, quasi come un atto di "volontariato", quindi con un forte senso di responsabilità. Tuttavia, questa rimane l'eccezione. A proposito di responsabilità, mi corre obbligo raccontare di riunioni di coordinamento tra periti (riguardanti casi con decine di vittime) annullate perché il coordinatore doveva correre in qualche studio televisivo, dopo aver trascorso l'intera mattinata di riunione in contraddittorio, distratto, e chattando con il giornalista che organizzava urgentemente la puntata. Analoga mancanza di senso di responsabilità è testimoniata da un altro episodio. Ho assistito alla rimozione surrettizia di interi paragrafi di una perizia estremamente tecnica in quanto non di dominio da parte del perito, il quale, non specificatamente formato sull'argomento, probabilmente temeva che la necessità di includere un altro esperto nel team avrebbe potuto eclissare un po' la sua visibilità nel contesto "vetrina". Anche questa perizia entrava nel merito di un disastro con molte vittime.

Oltre alle sfide affrontate dai periti, è importante considerare anche le dinamiche che coinvolgono i consulenti tecnici di parte, che presentano un insieme unico di problemi e responsabilità. A proposito dei C.T.P, quindi, devo riportare qualche episodio utile ad inquadrare bene il contesto professionale.

Rispetto alle indagini sui disastri avvenuti anni fa, la nuova generazione di consulenti ha apportato cambiamenti significativi nella gestione del contraddittorio. Essere selezionato come consulente di parte in un caso di rilevanza nazionale è diventato l'obiettivo di molti accademici e professionisti, attratti dai considerevoli guadagni potenziali. Tuttavia, ho osservato che si è ridotta la tendenza a scrivere relazioni di parte e che i consulenti tecnici di parte (C.T.P.) tendono a fatturare "a giornate", basandosi sui giorni in cui si svolgono le attività peritali in contraddittorio. Questa modalità di fatturazione implica che i consulenti non vengano remunerati per le ore dedicate allo

studio del caso, e di conseguenza, partecipino meno attivamente all'indagine. Va da sé che ci si deve comunque inventare un ruolo, per giustificare la propria presenza ed il proprio cachet.

A proposito della filosofia dell'"inventarsi il ruolo", al grido di "facite ammuina", non dimenticherò mai un episodio eclatante. In un importante caso nazionale con molte vittime, fu coinvolto un consulente esperto in sensori di sorveglianza, noto in quanto aveva lavorato su casi di cronaca nera. Durante una riunione, il consulente descrisse un problema con un microfono che captava suoni molto deboli, paragonandolo a un microfono avvolto in carta da regalo. Questo problema aveva reso i suoni di un incidente quasi inudibili, secondo quanto riferito dagli esperti.

Il focus delle discussioni successive, che coinvolgono sia consulenti tecnici di parte (C.T.P.) che periti, doveva essere su due sistemi di sicurezza che avevano fallito contemporaneamente in un impianto, causando conseguenze fatali. Tuttavia, per due riunioni, il dibattito si concentrò solo sulla questione del microfono "incartato", posto a 30 metri di altezza. È stata un'esperienza surreale ed ho atteso invano che qualcuno sdrammatizzasse dichiarando che si trattava di uno scherzo.

«È ovvio che la maggior parte degli incarichi riguarda l'analisi di fonti digitali come cellulari, computer personali e telecamere di sorveglianza. Spesso, la quantità di dati da queste fonti è soverchiante, rendendo necessario personale extra e l'uso di strumenti commerciali per l'estrazione e l'analisi, gestiti da un tecnico specificamente formato, quindi non accademico, ma costantemente aggiornato ed allenato in questi dispositivi.»

Alla fine, parlando con alcuni tecnici e consultando il fornitore, si scoprì che il problema era dovuto semplicemente a un cursore del volume spostato, una situazione già verificatasi in passato.

Mi sento obbligato a riferire pochi altri episodi davvero eccezionali per comprendere meglio il contesto. Un episodio riguarda un abile consulente, noto per il suo background tecnico-scientifico e particolarmente temuto per la sua competenza in procedura

penale. Durante una riunione peritale in ordine di incidente probatorio, in una fase intermedia che stava precedendo di mesi la consegna della perizia, questo consulente, da me soprannominato "Zenone", è riuscito a paralizzare il lavoro del collegio dei periti. In questa riunione, il cui ordine del giorno era la consegna per iniziare la discussione su materiale documentale appena ricevuto, Zenone ha deviato l'intera giornata di lavori dal punto previsto. Si è lamentato di non aver potuto preventivamente visionare il materiale, rendendosi quindi incapace di discuterne e trascinando tutti i presenti in una accesa discussione sulla procedura. Il che è ovviamente un paradosso, visto il punctum della riunione stessa che riguardava proprio la consegna.

Ottenuto un rinvio, nella successiva riunione, con lo stesso ordine del giorno, a pochi minuti dall'inizio Zenone ha chiesto di poter accedere ad una stanza riservata nello studio che ci ospitava. Qui ha intrattenuto una diversa videoconferenza per un altro cliente, riuscendo così a fatturare la stessa giornata a due diversi, ignari, indagati.

Zenone, persona certamente dotata di intelligenza molto fine, non ha mai fornito spunti al difficile lavoro dei periti. Il suo lavoro, infine, ha avuto come massima espressione lo sfruttamento delle fasi concitate delle convocazioni durante le udienze del giudice delle indagini preliminari. È riuscito a convincere i suoi colleghi periti di non essere stato convocato, dai suoi avvocati, per intervenire sulla perizia il giorno e nella sede prevista. Ha anche postato immagini di sé con la sua famiglia, la sera prima, a 300 km dal luogo dove si teneva il processo. Sfruttando quel po' di confusione inevitabile in queste circostanze e facendo leva sulla deontologia tra colleghi, è quindi riuscito ad attaccare la perizia in assenza degli autori.

Questo contesto, evidentemente promiscuo, accentua la sua pericolosità se si considera che i periti o i C.T. delle procure sono in numero decisamente esiguo rispetto alla domanda e che i giudici non hanno accesso ad un albo nazionale magari suddiviso per competenze concrete e si devono rivolgere a suggerimenti tra colleghi oppure ai nomi "della televisione".

Cerchiamo ora di dare un ordine a questi pensieri che potrebbero apparire sparsi, ed arrivare al punto di questa mia testimonianza, molto personale, con una lista concisa:

- La Digital Forensics non è solo cellulari e pc ma anche accident investigation "cyber-physical";

- Gli specialisti coinvolti possono essere professionisti o personale preso in prestito dal mondo accademico o della ricerca;
- Attività di Digital Forensics in ambito infrastrutture critiche richiede molto tempo ed un approccio multidisciplinare e di vera e propria ricerca;
- Attività di Digital Forensics nell'ambito più diffuso richiede costose licenze software e spese di gestione elevate;
- Quando purtroppo l'incarico riguarda un disastro, vengono approntate indagini ministeriali e penali, con le prime che dipendono dalle seconde o ne vengono comunque limitate.

A proposito delle indagini ministeriali:

- Hanno come focus il prevenire futuri incidenti;
- Alcune competenze devono essere acquisite da fuori, soprattutto per quanto concerne le competenze "digitali";
- Sono limitate nel tempo a causa del contesto internazionale nel quale si trovano ad operare;
- Non hanno pieno accesso al fascicolo dell'indagine giudiziaria e non partecipano a tutte le riunioni peritali.

Quindi...

A proposito delle indagini penali:

- Hanno come focus l'accertamento delle responsabilità;
- Tutte le competenze tecniche provengono da consulenti: professionisti o provenienti dall'accademia;
- Sono meno limitate nel tempo ma subiscono pressioni dagli organi di stampa, a volte polarizzati e polarizzanti;
- De facto sono essenziali anche per la più completa ricostruzione e quindi per evitare ulteriori disastri;

- Vengono spesso limitate dai consulenti di parte che cercano di buttarla sul lato “procedurale”.

A proposito dei periti che provengono dall’accademia:

- Dovrebbero essere più indipendenti come forma mentis, non provenendo da ambienti professionali super-specifici. In realtà c’è sempre il rischio di forme, anche inconsapevoli, di sudditanze nei confronti di colleghi dello stesso settore scientifico disciplinare e concorsuale;
- Per un lavoro di qualità dovrebbero avere una compensazione “accademica” oltre che avere uno stipendio già garantito (almeno finché il dipartimento lo consente e tollera);
- Hanno certo bisogno di colleghi “professionisti” che possiedono strumenti ma soprattutto formazione e training per il lato “consumer Digital Forensics” cioè telefonini, pc, videocamere, eccetera;
- Non hanno esperienza lato procedura e si lasciano ostacolare da colleghi più smaliziati.

A proposito dei consulenti “professionisti”:

- Devono rinunciare a stipendi da migliaia di euro al giorno per 4/8 euro l’ora a vacazione;
- Sostengono spese davvero ingenti;
- I mancati guadagni vengono quindi compensati con visibilità mediatica che si trasformi in nuovi clienti;
- Questo fa sì che, in indagini delicate, vengano trattenuti ruoli chiave da professionisti non specificatamente competenti e che quindi preferiscono non coinvolgere altri colleghi più specializzati;
- Anche tra i professionisti della Digital Forensics, a volte, si crea un circolo chiuso, c'è forse un po’ troppo reciproco rispetto tra consulenti.

A proposito dei consulenti di parte:

- Recentemente ho osservato casi in cui questi hanno completamente rinunciato a partecipare costruttivamente alle indagini;
- Talvolta sembra che il loro ruolo sia unicamente rallentare/impedire i periti;
- Ad ogni modo non hanno, da mandato, nessun interesse nel risolvere il caso in ottica “sicurezza”;
- Fanno parte del medesimo circolo chiuso: è accettabile che due professionisti si scontrino, a ruoli invertiti tra quelli d’ufficio e di parte, in due casi contemporanei di rilevanza nazionale? Questo, ovviamente, vale allo stesso modo per professionisti ed accademici.

Quindi? Alcune idee:

- Agli accademici dovrebbe essere riconosciuto un incentivo di ricerca, nel senso che gli anni spesi a lavorare su di un caso possano essere valutati come pubblicazioni, se la perizia contiene lavori rilevanti in ambito scientifico;
- Separazione delle carriere tra periti e consulenti di parte per quanto concerne le attività di analisi (ma non necessariamente quelle di acquisizione della prova);
- Adeguamento dei compensi dei periti, ovviamente;
- Affiancare ai collegi peritali una figura esperta e titolata di diritto. Per garantire l’indipendenza dei periti, ho sempre osservato che le comunicazioni col tribunale si riducono allo stretto necessario. Nei casi più intricati, suggerisco però di permettere ai collegi peritali di potersi avvalere delle competenze di un giurista, da includere nel team;
- Un coordinatore del collegio peritale proveniente da un’agenzia governativa specializzata (oppure proveniente dal mondo militare, quando possibile). Idealmente, per mitigare prontamente le aberrazioni che possono incidere sul corretto svolgimento dell’attività giudiziaria penso debba essere istituito un servizio nazionale che raggruppi personale scientificamente, tecnicamente e moralmente idoneo a supportare tribunali e procure nei casi giudiziari che richiedono competenze di alto livello. Gli afferenti non dovrebbero sviluppare rapporti privatistici di consulenza.

CONCLUSIONE

In conclusione, la disciplina, o il mestiere, della Digital Forensics in Italia si trova ad un bivio critico. Mentre il campo si espande e diventa sempre più rilevante nel contesto legale e giudiziario, emergono sfide significative legate alla professionalità, alla formazione e alla gestione etica delle indagini. Lo studio della sovrapposizione tra errori umani e problemi tecnici, la mancanza di una chiara separazione delle carriere tra periti e consulenti tecnici di parte, e le pressioni economiche e mediatiche su questi professionisti richiedono un'attenzione urgente.

Le soluzioni proposte, tra cui l’introduzione di incentivi di ricerca per gli accademici, la separazione delle carriere, l’adeguamento dei compensi e l’integrazione di competenze giuridiche nei team peritali, mirano a creare un ambiente più equilibrato e funzionale. Inoltre, l’istituzione di un servizio nazionale per supportare tribunali e procure potrebbe garantire un’indipendenza e un’efficacia maggiore nelle indagini.

Affrontare queste sfide non sarà semplice, ma è essenziale per garantire che la Digital Forensics in Italia possa continuare a svolgere un ruolo cruciale nella giustizia e, soprattutto, nella sicurezza pubblica.

CLOUD COMPUTING: VERSO NUOVE TUTELE PER IL BUSINESS CONSUMER

Rita Eva Cresci, Iusintech

ABSTRACT

Con la scalata del Cloud Computing e della moltitudine di servizi offerti attraverso questa rivoluzionaria risorsa, l'impatto della standardizzazione tecnologica sull'impresa, specie quella italiana, ha determinato profili di preoccupante asimmetria contrattuale che vanno compensati con una revisione di approccio sia da parte del fruitore che a livello regolatorio, per garantire nuove tutele rispetto alla vulnerabilità e ai rischi assunti una volta migrati sulla nuvola.

Occorre, in buona sostanza, rimettere al centro autodeterminazione e libertà negoziale come valori imprescindibili anche del mercato digitale.

Sebbene con il Digital Service Act (DSA) e il Digital Market Act (DMA), l'Unione Europea stia provando a tratteggiare una nuova costituzione dedicata all'ecosistema digitale, anteponendo la potenza del diritto a quella prettamente tecnologica – con il preciso fine di contenere lo strapotere dei cd. gatekeeper, compresi, senza dubbio, i fornitori di infrastrutture cloud –, nella pratica commerciale siamo ancora piuttosto lontani dall'auspicato bilanciamento di potere a tutto sfavore dell'utenza, a prescindere dalle sue dimensioni.

Giova dunque soffermarsi sull'approfondimento di alcuni aspetti critici della contrattualistica di settore (di matrice schiettamente unfair, quali clausole vessatorie, pratiche commerciali scorrette, ingannevoli e aggressive) entrati nel mirino delle Authorities Antitrust, potenzialmente in grado di mettere in ginocchio, se non

opportunamente disinnescati con puntuali cautele di governance, anche organizzazioni complesse e ben strutturate.

IL CONTESTO

Mentre le applicazioni informatiche garantite dalla tecnologia Cloud si sono fatte strumenti sempre più irrinunciabili per l'impresa, i poteri sulle risorse e sulle funzionalità IT sono molto cambiate rispetto al passato.

Le facoltà di interazione dell'utilizzatore rispetto ai servizi di Cloud Computing non sono più quelle che aveva il committente "dominus" rispetto al frutto del lavoro del suo programmatore, in ragione del fatto che, nell'era della nuvola, il rapporto tra le parti non trova più la sua determinazione in un incarico ad hoc, ma viene di norma regolato attraverso una proposta generalista e massificata coordinata secondo un complesso di clausole "preconfezionato", per lo più di matrice anglosassone, rilasciato, per lo più, online da potenti player multinazionali.

«In capo al Business Consumer, si pone dunque, indubitabilmente, un notevole sforzo pre-negoziale, mirato a ricostruire l'insieme dell'impianto della struttura contrattuale applicabile ai servizi di interesse, nonché a decifrare la gerarchia intrinseca alle disposizioni contenute nei vari documenti che gli vengono sottoposti.»

La maturazione delle tecnologie, e un nuovo utilizzo di Internet come strumento abilitante l'interazione delle risorse, stanno dunque alla base della modifica sostanziale di domanda e offerta nell'Industry ICT (Information and Communication Technology). Il prodotto di questo cambiamento è una nuova filiera di settore, quella del Cloud Computing appunto, che si sostanzia nella standardizzazione dei servizi informatici di commodity più disparati (computazionali, infrastrutturali, di memorizzazione, di archiviazione, di intrattenimento, di protezione, gestionali ecc.).

La smaterializzazione documentale, la centralità del dato, la delocalizzazione di molte attività, la necessità di operare da remoto e, contestualmente, in ambienti condivisi,

hanno spinto il mercato verso il Cloud a ritmo vertiginoso (solo in Italia con un +19% il mercato del Cloud nel 2023 vale oltre 5,5 miliardi di euro, secondo l'ultimo Report dell'Osservatorio Cloud Transformation del POLIMI) con la conseguente proliferazione di utenti sempre più attenti alla performance tecnica a basso costo ma contestualmente vulnerabili e distratti rispetto ai termini di una negoziazione che, pur presentandosi apparentemente molto accessibile, cela in realtà aspetti di indubbia pericolosità.

LA STRUTTURA DEL CONTRATTO DI CLOUD COMPUTING

Sempre facendo riferimento ai servizi Cloud offerti dai grandi provider americani, quali Google, Amazon, Microsoft, ecc., la struttura del contratto segue un modello Common Law, costituito per lo più da quattro diversi documenti:

a. Terms of Service (ToS o CGC): contiene le definizioni iniziali degli elementi del contratto e le condizioni generali di servizio (durata, corrispettivo, modalità di erogazione, ipotesi di risoluzione e di recesso, ecc. in cui è solitamente esclusa l'obbligazione di risultato);

b. Service Level Agreement (SLA): precisa il livello qualitativo e quantitativo dei servizi erogati, che il provider si impegna a mantenere e in relazione ai quali l'utente si impegna a pagare un corrispettivo;

c. Acceptable Use Policy (AUP): regola gli usi consentiti all'infrastruttura hardware e software messa a disposizione dell'utente o tutte le ipotesi in cui il mancato rispetto di detti limiti giustifica l'immediata sospensione o interruzione del servizio;

d. Privacy Policy: stabilisce (unilateralmente) le modalità con cui il provider si impegna a trattare i dati immagazzinati dell'utente.

In capo al Business Consumer, si pone dunque, indubitabilmente, un notevole sforzo pre-negoziale, mirato a ricostruire l'insieme dell'impianto della struttura contrattuale applicabile ai servizi di interesse, nonché a decifrare la gerarchia intrinseca alle disposizioni contenute nei vari documenti che gli vengono sottoposti. In aggiunta, va ricordato, che è frequente all'interno di questi modelli trovare dei richiami URL che rinviano per relazione ad altri testi contrattuali che diventano ugualmente vincolanti

per l'utente, ponendolo, se possibile, in posizione ancora più svantaggiata e vulnerabile quanto alla ricostruzione dei rischi assunti.

PRATICHE COMMERCIALI SCORRETTE, INGANNEVOLI E AGGRESSIVE

La disciplina delle pratiche commerciali scorrette è dettata dagli artt. 18-27 quater del Codice del consumo (d.lgs. n. 206/2005), a cui si è affiancata la direttiva di modifica (UE) 2019/216, la cd. Direttiva Omnibus, entrata in vigore lo scorso aprile, che ha come obiettivo quello di migliorare la conoscenza dei diritti dei consumatori stessi nonché quello di rafforzare l'attuazione dei diritti medesimi e dei rimedi ad essi collegati.

«Il divieto generale di pratiche commerciali scorrette si fonda su due requisiti cumulativi: la contrarietà della pratica alla diligenza professionale e la sua idoneità a falsare in misura rilevante il comportamento economico del consumatore medio, ovvero "l'impiego di una pratica commerciale idonea ad alterare sensibilmente la capacità del consumatore di prendere una decisione consapevole, inducendolo pertanto ad assumere scelte di natura commerciale che non avrebbe altrimenti preso".»

In forza di detto contesto regolatorio, si definisce aggressiva e sleale quella pratica commerciale che, tramite molestie, coercizione o indebito condizionamento (anche indiretto e astratto), comprometta in maniera significativa la libertà di scelta del consumatore medio e lo induca ad assumere una decisione di natura commerciale che altrimenti non avrebbe assunto.

La previsione del divieto di pratiche commerciali sleali si estende a "prima, durante e dopo un'operazione commerciale relativa a un prodotto" (art. 19 co. 1 C. cons.), mentre per quanto attiene all'ambito di applicazione soggettivo, la normativa lo circoscrive ai soli rapporti business to consumer (B2C), comprendendo però in questo confine anche le micro-imprese (il distinguo applicativo è di assoluta rilevanza, considerato che in Italia le micro imprese sono 4,1 milioni, ovvero il 95% del totale e attività imprenditoriali fino a nove addetti danno lavoro a quasi 7,6 milioni di cittadini, pari al 44,5% degli occupati).

L'impianto della disciplina comprende una clausola generale di scorrettezza, due disposizioni specifiche che riguardano le distinte categorie di pratiche "ingannevoli" e "aggressive" e due "liste nere" di condotte definite sempre scorrette sulla base di un giudizio preventivo compiuto dal legislatore.

Il divieto generale di pratiche commerciali scorrette si fonda su due requisiti cumulativi: la contrarietà della pratica alla diligenza professionale e la sua idoneità a falsare in misura rilevante il comportamento economico del consumatore medio, ovvero "l'impiego di una pratica commerciale idonea ad alterare sensibilmente la capacità del consumatore di prendere una decisione consapevole, inducendolo pertanto ad assumere scelte di natura commerciale che non avrebbe altrimenti preso".

Nel contesto che ci occupa, il bene garantito dalla disposizione è dunque, incontrovertibilmente, la libertà negoziale nel mercato digitale.

La clausola generale si articola, poi, in due distinte tipologie: le pratiche ingannevoli (a loro volta distinte in azioni e omissioni ingannevoli) e le pratiche aggressive.

Per quanto attiene alle pratiche ingannevoli, il Codice del Consumo distingue tra "azioni" ed "omissioni" ingannevoli. Per le pratiche di tipo commissivo, l'azione ingannevole può integrare una pratica commerciale scorretta quando "contiene informazioni non rispondenti al vero" o "seppure di fatto corretta, in qualsiasi modo, anche nella sua presentazione complessiva, induce o è idonea ad indurre in errore il consumatore medio" (art. 21, comma 1, C. cons.). In entrambi i casi, si richiede che la pratica induca o sia idonea a indurre il consumatore "ad assumere una decisione che non avrebbe altrimenti preso" (c.d. materiality test).

Dalla disposizione si evince con chiarezza come l'idoneità a indurre in errore il consumatore implichi una valutazione omnicomprensiva della pratica, dal momento che – al di là della veridicità o meno delle informazioni trasmesse – elementi come la presentazione del messaggio, il contesto della comunicazione, le sue modalità di diffusione e la sua veste grafica possono incidere sull'impatto e sulla percezione del messaggio, rivelandosi quindi potenzialmente distorsivi e alterativi della libertà di scelta del consumatore.

La disciplina in esame annovera non solo l'omissione di informazioni "rilevanti" che il fruitore ha bisogno di conoscere per prendere decisioni consapevoli di natura

commerciale, ma anche l'occultamento e il modo oscuro, incomprensibile, ambiguo o intempestivo con cui il professionista fornisce informazioni rilevanti al consumatore (art. 22 C. Cons.). In entrambi i casi, tali condotte sono suscettibili di divieto purché inducano o siano idonee ad indurre il consumatore medio ad assumere una decisione commerciale che altrimenti non avrebbe preso.

A questo primo genere di pratiche commerciali scorrette – ingannevoli – sono sembrate ascrivibili le condotte commerciali di Google, Apple e Dropbox a seguito delle istruttorie di AGCOM del febbraio 2022 che hanno portato alle maxi multe pari a 20 milioni di euro, motivate nella "mancata o inadeguata indicazione dell'attività di raccolta e utilizzo a fini commerciali dei dati forniti dall'utente". Lo stesso dicasi – nel caso specifico di Dropbox – per "l'aver omesso di fornire all'utente, in maniera chiara e immediatamente accessibile, le informazioni sulle condizioni, sui termini e sulle procedure per recedere dal contratto e per esercitare il diritto di ripensamento" oltre alle indicazioni necessarie per consentire l'agevole ricorso a "meccanismi extra-giudiziali di conciliazione delle controversie, cui il professionista sia soggetto".

«Laddove le pratiche ingannevoli assumono una portata decettiva rispetto alla decisione commerciale del consumatore, influenzandone il processo di formazione della volontà, vengono definite aggressive e hanno una valenza estorsiva più generale sulla libertà di scelta del consumatore – che rappresenta il bene giuridico protetto dalla disciplina in esame – sfruttandone le debolezze caratteriali, emotive e culturali.»

Laddove le pratiche ingannevoli assumono una portata decettiva rispetto alla decisione commerciale del consumatore, influenzandone il processo di formazione della volontà, vengono definite aggressive e hanno una valenza estorsiva più generale sulla libertà di scelta del consumatore – che rappresenta il bene giuridico protetto dalla disciplina in esame – sfruttandone le debolezze caratteriali, emotive e culturali.

Dal tenore dell'art. 24 C. Cons., si evince come le pratiche aggressive si compongano di due elementi costitutivi: uno di carattere strutturale, relativo al mezzo utilizzato (il

rimando questo caso è alla struttura tipica del contratto di Cloud Computing, costituito da vari documenti e allegati tecnici, scritti in inglese e fitti di rimandi attraverso URL ad altri documenti ugualmente vincolanti per l'utente, senza alcuna effettiva organizzazione per argomento che ne agevoli la comprensione) ed uno di carattere funzionale, rappresentato dall'attitudine della pratica ad indurre il consumatore ad assumere una decisione commerciale che non avrebbe altrimenti preso.

Quanto ai criteri di valutazione dell'aggressività di una pratica commerciale, ciò che rileva, anche ai fini della presente analisi contrattuale nel mercato del Cloud, è lo sfruttamento di una posizione di potere rispetto al consumatore per esercitare una pressione, anche senza il ricorso alla forza fisica o la minaccia, in modo da limitare notevolmente la capacità del consumatore di prendere una decisione consapevole (art. 18, lett. l C. Cons.).

In proposito, è stato opportunamente precisato che per decisione consapevole non si intende la decisione cosciente (o informata) ossia la rappresentazione corretta delle caratteristiche del prodotto che si intende acquistare, bensì la scelta di acquisto presa in assenza di paure, pressioni o condizionamenti di sorta.

Anche in questo caso il valore da tutelare è sempre quello della libera scelta del consumatore digitale. Invero, lo sfruttamento della suddetta posizione di potere sfocia in una pressione precontrattuale o contrattuale del fornitore volta a trarre vantaggio da una condizione di vulnerabilità – economica, professionale, psicologica – del consumatore e a compromettere la sua capacità di decidere in conformità ai propri reali interessi e bisogni.

In merito alle indagini avviate da AGCOM di cui si è parlato nei paragrafi precedenti, ciò che nello specifico è stato contestato a Google e Apple come pratiche ritenute aggressive è la mancanza di chiarezza di informazioni in merito alla raccolta dati, nella fase di creazione dell'account, ai fini commerciali da un lato e dall'altro la preimpostazione del consenso dell'utente alla raccolta e all'utilizzo delle informazioni personali a fini commerciali, in aperto spregio anche a quanto stabilito sul consenso libero ed informato ex art 7 GDPR.

LE CLAUSOLE VESSATORIE

Infine, la disciplina normativa delle clausole vessatorie varia a seconda della natura dei contraenti: si applica la normativa codicistica (artt. 1341-1342 c.c.) nel caso di contratti conclusi tra professionisti o imprenditori (B2B), mentre nei rapporti tra professionisti e consumatori (B2C) si applica, come abbiamo già precisato, la disciplina consumeristica.

La vessatorietà di una clausola viene valutata alla luce di due criteri: il principio generale espresso dall'art. 33, co. 1, C. Cons., secondo cui si considerano vessatorie le clausole che malgrado la buona fede, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto – con ciò intendendosi uno squilibrio di tipo "normativo" e non meramente economico – tenendo conto della natura del bene o del servizio oggetto del contratto, sulla base delle circostanze esistenti al momento della sua conclusione e delle altre clausole contenute nello stesso ovvero in altro contratto ad esso collegato o da cui dipende (art. 34 C. Cons.). Per clausole di questo tipo, l'accertamento è condotto dal giudice in relazione al caso concreto, e l'onere della prova incombe sul consumatore, mentre per le fattispecie tipizzate (di cui agli artt. 33 co. 2 e 36 co. 2 C. Cons.) il legislatore ha già effettuato a priori una presunzione di vessatorietà: detta presunzione è quindi relativa nel primo caso e assoluta nel secondo.

Nello specifico, l'art. 33, co. 2., contiene un elenco non tassativo delle clausole che si presumono vessatorie fino a prova contraria (c.d. lista grigia). La presunzione di vessatorietà comporta che, in difetto di prova contraria da parte del fornitore, le suddette clausole siano nulle (c.d. vessatorietà iuris tantum, ossia presunta sino a prova contraria).

Tra queste, compaiono alcune delle clausole oggetto di contestazione da parte di AGCOM e autorità assimilabili a carico delle Big Tech, nello specifico quelle "che hanno per oggetto o per effetto di consentire al fornitore di modificare unilateralmente le clausole del contratto, ovvero le caratteristiche del prodotto o del servizio, senza un giustificato motivo indicato nel contratto stesso" (art. 33, co. 2, lett. m). Recentemente anche il regolatore britannico delle comunicazioni Ofcom[1] ha deciso di "riferire" il mercato della

1 *https://www.corrierecomunicazioni.it/brand/Ofcom*

fornitura di servizi di Public Cloud all'Autorità Antitrust[2] (CMA) per ulteriori indagini, dopo aver identificato pratiche che rendono difficile per i clienti britannici cambiare fornitore o utilizzarne diversi.

CONCLUSIONI

I profitti stellari dei player del settore hanno determinato in breve tempo leadership incontrastabili ed una certa tendenza "compatta" a derive di privatizzazione del contratto, esternate in una rigidità nel modello di business quasi ferrea, che a fronte dell'irrinunciabilità dei servizi resi, non sarà facile scardinare, pur risultando spesso incompatibili con i principi fondamentali del nostro ordinamento giuridico, davanti ai quali l'autonomia negoziale trova il suo limite (ad esempio nelle norme imperative della disciplina che tutela la libera concorrenza e il mercato).

A prescindere da tutte le norme, regolamenti, direttive citate precedentemente, un'importante arma a disposizione del business consumer, in grado di preservarlo da pericoli frequenti come quello del vendor-lock-in (ovvero l'impossibilità di cambiare provider senza pesanti conseguenze finanziarie e/o organizzative) resta quella del preliminare "vaglio strategico" realizzato attraverso un'analisi che non prenda in esame solo la performance tecnica ma consideri altresì la reale portata delle obbligazioni assunte e le effettive responsabilità allocate in capo alle parti attraverso opportuno confronto multidisciplinare, allargando, almeno per alcuni servizi di base, la potenziale rosa di fornitori anche alle ormai eccellenti realtà europee in grado di garantire maggiori margini di personalizzazione, nella certezza del rispetto di tutto l'impianto normativo sul trattamento dei dati, così come della disciplina consumeristica.

2 https://www.corrierecomunicazioni.it/tag/antitrust

FACEBOOK E PAYWALL, L'ESATTO VALORE DELLA PUBBLICITÀ PROFILATA. O NO?

Marco Cuniberti, Costa e Cuniberti Avvocati Associati

E così il gran giorno è arrivato.

Disabilitando i cookie non necessari (mentre lo facevo, ho scoperto che, curiosamente, Meta mi aveva di nuovo abilitato e quelli facoltativi, ovviamente senza che io lo sapessi o lo volessi: ma vabbè), sia sul computer che sullo smartphone è comparso il paywall di Meta, che mi comunicava che, da quel momento, se non pagavo l'abbonamento (9,99 euro sul computer, 13,99 sullo smartphone al mese, per un totale di annuale di 155,88 euro all'anno) o non acconsentivo a ricevere pubblicità profilata, non avrei più potuto utilizzare Facebook.

Facebook ha tutto il diritto di farsi pagare per il servizio che offre, per cui mi pare sbagliato gridare allo scandalo affermando che, se non ci si può permettere economicamente l'abbonamento, si è "costretti" a cedere i propri dati personali, così rinunciando a un diritto assoluto come quello alla protezione dei dati personali.

Il ragionamento sembra erroneo alla base, in quanto, non trattandosi di un servizio essenziale o che comunque debba essere garantito a tutti perché necessario (anzi, se posso dire, è inutile – se non addirittura dannoso – tanto che si parla spesso di vietarlo ai minori), c'è una terza scelta possibile, cioè non fruire di questo servizio, assolutamente voluttuario.

Nessuno si è mai lamentato del fatto che l'acquisto di un giornale cartaceo sia a pagamento; o che andare in palestra, sciare, andare al cinema o abbonarsi a Sky abbia un costo.

Se tutti questi servizi ci proponessero, in alternativa al pagamento del prezzo in denaro, la possibilità alternativa di pagare cedendo alcune nostre informazioni (più o meno invasive: ma questo è un altro discorso), si concretizzerebbe di colpo una discriminazione tra ricchi e poveri? Ovviamente no.

Preso da solo, questo ragionamento lo ritengo, ripeto, sbagliato e capzioso.

E infatti, alcune DPA (cioè le Autorità di controllo nazionali) che hanno già deciso su casi del genere hanno propeso per l'ammissibilità del sistema (perlomeno in via astratta, come d'altronde previsto espressamente da più norme, anche europee), ma a determinate e rigide condizioni (quasi mai riscontrate in concreto), tra cui la congruità del prezzo richiesto in denaro.

«Facciamoci una domanda: sugli svariati milioni di utenti italiani, quanti pensiamo che stipuleranno l'abbonamento a pagamento di Facebook per oltre 150 euro all'anno?»

È qui (e non sulla astratta ammissibilità del nuovo sistema alternativo di pagamento), che ci si bisogna concentrare, per valutare la legittimità o meno della condotta di Meta.

Facciamoci una domanda: sugli svariati milioni di utenti italiani, quanti pensiamo che stipuleranno l'abbonamento a pagamento di Facebook per oltre 150 euro all'anno?

Se è possibile che qualcuno davanti all'alternativa decida di non usare più il social network (anche se sarà una percentuale irrisoria), penso che gli utenti "consumer" (con ciò intendendo coloro che usano il social network solo per diletto personale, senza alcuno scopo professionale) che andranno a pagare tale prezzo si potranno contare forse sulle dita di una mano e probabilmente sarebbe bene che si facciano vedere da uno bravo.

Il vero punto è che non pare credibile che la sola pubblicità profilata valga veramente 155,88 euro a persona all'anno (da moltiplicare per circa 3 miliardi di utenti), in quanto significherebbe che, dalla sola pubblicità profilata (che non è l'unica fonte di guadagno per Meta, anzi) – e solo per Facebook – essa incasserebbe in un anno circa 470 miliardi di euro, cioè oltre 500 miliardi di dollari.

Il che, malgrado la mia immensa stima imprenditoriale per Zuckerberg e soci, non è possibile, se è vero che il fatturato mondiale di tutta la pubblicità online (ma proprio tutta, compresi gli altri social network di Meta, TikTok, YouTube, Google e gli altri motori di ricerca, ecc.) è pari a 408 miliardi di dollari[1] e lo stesso bilancio di Meta indica, come ricavi pubblicitari di tutte le sue attività (di cui Facebook rappresenta solo una parte), circa 100 miliardi di dollari.

E ripeto che si tratterebbe solo dei guadagni provenienti dalla pubblicità profilata, perché Meta dichiara espressamente che, pagando l'abbonamento, i dati personali "non saranno usati per le inserzioni": per cui continueranno a essere utilizzati per tutte le ulteriori finalità, esattamente come prima.

E allora perché Meta avrebbe stabilito un prezzo palesemente fuori mercato e, apparentemente, sproporzionato rispetto al guadagno derivante dalla monetizzazione dei dati con la pubblicità profilata (operazione, quest'ultima, oltretutto molto più onerosa)?

Non vuole guadagnare direttamente denaro?

Oppure, forse, come ben evidenziato da NOYB davanti all'autorità austriaca, in un caso simile (anche se si trattava del paywall di un giornale), il prezzo sarebbe volutamente sproporzionato proprio perché gli utenti non scelgano quest'opzione?

Se la risposta fosse, come pare probabile, la seconda, occorrerebbe che Meta ci spiegasse il perché.

Ci sarebbe in ogni caso un grosso problema di liceità, in quanto, come stabilito dall'autorità austriaca nel caso citato (ma non solo), l'utilizzo dei dati personali come metodo alternativo di pagamento del prezzo di un servizio può essere ammissibile soltanto se il prezzo in denaro richiesto sia congruo rispetto al guadagno derivante dalla monetizzazione dei dati richiesti in alternativa: in caso contrario, cioè nell'ipotesi di prezzo sproporzionato, l'utente sarebbe spinto a pagare tramite la cessione dei suoi dati illecitamente, con un sistema subdolo e quindi illecito.

La mancanza di trasparenza (chi ha tempo da perdere, può provare a capire qualcosa

---

1 *Come spiegato qui: https://tinyurl.com/53p8nvjr*

della mastodontica e criptica informativa, con buona pace dell'art. 12 GDPR), in un servizio che ormai è acclarato essere a pagamento da sempre, comporta poi la necessità di un nuovo assessment anche a livello di conformità della normativa a tutela dei consumatori, con ulteriori criticità.

Restano comunque sul piatto tante altre questioni (che qui non affronterò), tra cui quella della posizione dominante (quantomeno, visti i ricavi pubblicitari sul totale mondiale) di Meta sul mercato dei social network, vista come fumo negli occhi dalle DPA europee (CNIL in primis) per valutare la liceità di questo sistema di pagamento di servizi online, in quanto influirebbe sulla effettiva libertà del consenso (anche se si comincia a ragionare, se realmente fossimo di fronte a trattamenti la cui monetizzazione fosse congrua rispetto al prezzo in denaro chiesto in alternativa, ad una base giuridica diversa dal consenso, cioè quella prevista dalla lettera B dell'art. 6 GDPR).

«Oppure, forse, come ben evidenziato da NOYB davanti all'autorità austriaca, in un caso simile (anche se si trattava del paywall di un giornale), il prezzo sarebbe volutamente sproporzionato proprio perché gli utenti non scelgano quest'opzione? Se la risposta fosse, come pare probabile, la seconda, occorrerebbe che Meta ci spiegasse il perché.»

Ma sotto questo punto di vista, il vero problema, a mio modesto avviso, resta il fatto stesso che sussista una posizione quasi monopolistica sul mercato globale, con un social network da 3 miliardi di iscritti nelle mani di un solo soggetto, che perdipiù possiede anche altri due dei quattro social network più diffusi al mondo, cioè Instagram (1,386 miliardi di utenti a gennaio 2023) e WhatsApp (che ormai è appunto considerato un social network, con 1,6 miliardi di utenti alla stessa data).

Ed è quindi a livello di antitrust e tutela della concorrenza che, forse, andrebbe risolto il problema, prima di giudicare la liceità del mezzo di pagamento.

KPI E LEGAL TECH TOOLS: MISURARE IL VALORE CREATO DAL DIPARTIMENTO LEGALE È OGGI POSSIBILE

Alessandro Del Bono, Elena Armini e Annalisa Olivieri, Deloitte Legal

È ormai consolidato il ruolo chiave dei dipartimenti legali nell'incrementare il valore delle organizzazioni aziendali. Il General Counsel è stato all'origine risk mitigator, poi business partner ed è arrivato il tempo di essere value creator, adottando le migliori strategie per fornire prestazioni di qualità da un lato e perseguire il contenimento dei costi dall'altro. Ma è possibile misurare il valore che un dipartimento legale apporta all'azienda? Sì, attraverso l'implementazione di KPI specifici per la funzione legale che siano in grado di catturarne il valore generato.

I KPI sono – letteralmente – indicatori chiave di prestazione, cioè indici di performance, valori misurabili che dimostrano l'efficacia e l'efficienza con cui un'azienda, un dipartimento o un settore valutano il raggiungimento del successo negli obiettivi prefissati. I KPI non sono dei valutatori delle prestazioni, ma dei misuratori che, se correttamente utilizzati, restituiscono informazioni immediate e oggettive sull'andamento del settore esaminato. Per fare in modo che funzionino correttamente è, quindi, necessario che siano scelti accuratamente e correlati agli obiettivi di business, mutando pertanto in base alla singola organizzazione e agli specifici obiettivi che si intende perseguire; invero, non esistono dei KPI standard validi per tutti, anzi, anche all'interno dello stesso contesto accade spesso che le metriche chiave legate ai KPI possano mutare nel tempo. Le più comuni misure correlate ai KPI sono di tipo economico e finanziario (es. l'ammontare delle vendite in euro o il livello di soddisfazione espresso dal cliente: alto, medio o basso). Tuttavia, se ci si concentra solo sugli indicatori di questo tipo si rischia di non catturare il valore generato dall'erogazione di prestazioni

caratterizzate da qualità, tempestività e soddisfazione del cliente interno, come ad esempio le prestazioni legali. Queste ultime, infatti, pur non avendo un impatto diretto sulle rilevazioni contabili, possono e debbono essere misurate e, di conseguenza, correttamente stimate attraverso una più ampia valutazione delle performance di una organizzazione.

La progettazione dei KPI specifici per il dipartimento legale richiede, pertanto, un approccio adattabile alle specificità dell'organizzazione e degli obiettivi, evitando soluzioni standard che potrebbero risultare inefficaci o controproducenti. L'approccio ideale all'individuazione e all'implementazione dei KPI specifici per la funzione legale tiene generalmente conto di quattro possibili problematiche:

1. Il tempo: il lavoro di misurazione deve essere fatto ciclicamente per ottenere dei punti di confronto omogenei e coerenti e deve sempre considerare eventuali variazioni ed aggiornamenti;
2. Le prestazioni: le performance del dipartimento legale non possono essere osservate in tempo reale e difficilmente potranno essere valorizzate nel breve termine. Per questo è importante poter valutare le prestazioni anche in termini di qualità e prioritizzazione;
3. La gestione: come qualsiasi altro dato è essenziale che la dashboard dei KPI del dipartimento legale sia precisa, aggiornata, coerente e completa, altrimenti l'analisi rischia di condurre a conclusioni non significative;
4. I dati: non tutti i dati sono informazioni e non tutti i numeri sono dati. Molto spesso, infatti, i numeri, se letti da soli, non riescono a restituirci una informazione completa ed è necessario, pertanto, leggerli insieme ad altri criteri ed indicatori.

Chiarito dunque che i KPI specifici del dipartimento legale possono rivelarsi un'utile risorsa in grado di rendere informazioni di valore sulla misurazione e sul raggiungimento degli obiettivi, la "golden question" è: come impostare i KPI del dipartimento legale?

Si può partire dalle seguenti domande:

1. Cosa misurare?

2. Quali sono le domande chiave per mettere a fuoco gli obiettivi della misurazione?
3. Quali metriche utilizzare per la misurazione?
4. Come effettuare la misurazione?
5. Come utilizzare le metriche?
6. Occorre un'analisi comparativa per utilizzare il dato?
7. Quanto impegno è richiesto per l'utilizzo delle metriche e la raccolta dei dati?
8. Ci sono tempistiche particolari?
9. Occorre un'analisi periodica per utilizzare il dato?
10. Ci sono aspetti pratici da tenere in considerazione?

La risposta a queste domande può costituire un valido punto di partenza per l'individuazione dei KPI per il dipartimento legale. È opportuno inoltre tenere in considerazione l'assunto per cui impostare un sistema di KPI costituisce solo la metà del percorso; l'altra metà, forse anche più importante della prima, è costituita dall'analisi e dall'interpretazione dei dati che determina quali azioni intraprendere per raggiungere gli obiettivi prefissati e migliorare la situazione attuale.

In questo contesto, l'utilizzo della tecnologia, se guidato dalle domande giuste, può facilitare la misurazione, ad esempio supportando il processo di monitoraggio e raccolta di dati, rendendo tale processo automatizzato, efficiente e trasparente e identificando attività ad alto volume e basso valore adatte all'automazione. I legal tech tools di ultima generazione possono, infatti, supportare concretamente la predisposizione e la condivisione della reportistica per la C-suite e per tutti gli stakeholder di riferimento. Se la selezione e l'implementazione della tecnologia sono state rigorose e riflettono la strategia che il dipartimento ha sviluppato per supportare l'organizzazione nel suo complesso, i vantaggi sono molteplici: migliora la gestione del rischio, incrementa l'efficienza, riduce gli errori umani, libera risorse da dedicare ad attività a maggior valore aggiunto. La tecnologia, di fatto, aiuta a monitorare l'evoluzione dei modelli operativi, supporta nella gestione dei carichi di lavoro delle persone e permette di ottimizzare i metodi di approvvigionamento nell'intreccio di team centrali e locali, Shared Service

Center e fornitori terzi. Ciò garantisce al General Counsel che le diverse questioni siano amministrate con trasparenza e che il rischio sia gestito correttamente, perché le attività non sono affidate ai membri del dipartimento legale sulla base di sensazioni, di ipotesi su chi sta facendo cosa. Il monitoraggio centrale della spesa consente altresì di generare metriche che permettono al General Counsel di dimostrare il valore aggiunto che il dipartimento legale trasformato sta fornendo, oltre che naturalmente a mantenere un più stretto controllo della spesa interna ed esterna. In tutti i casi, i risultati della valutazione possono essere utilizzati per migliorare continuamente il modo in cui l'organizzazione si avvale dei servizi legali, che siano forniti da interni o da terzi.

«È opportuno inoltre tenere in considerazione l'assunto per cui impostare un sistema di KPI costituisce solo la metà del percorso; l'altra metà, forse anche più importante della prima, è costituita dall'analisi e dall'interpretazione dei dati che determina quali azioni intraprendere per raggiungere gli obiettivi prefissati e migliorare la situazione attuale.»

Seguendo questo ragionamento ed intrecciando queste metriche con i livelli della Deloitte Legal House[1] (id est i) strategia, governance, ruoli e responsabilità; ii) servizi e compiti legali; iii) enablers), Deloitte Legal ha individuato 28 KPI legali specifici, volti alla misurazione del valore creato dal dipartimento legale a beneficio del dipartimento legale stesso e dell'intera organizzazione:

1. Budget,
2. Obiettivo delle attività;
3. Valore delle attività;
4. Efficienza ed innovazione;
5. Iniziative aziendali;

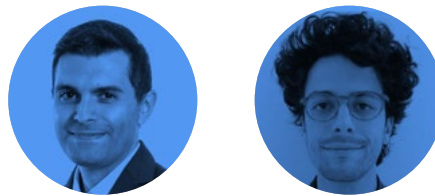
1 https://www2.deloitte.com/it/it/pages/legal/articles/time-to-build-legal-management-consulting-white-paper-2021---deloitte-ita.html

6. Collocazione del team;
7. Tipo di attività;
8. Metodi di lavoro;
9. Diversità e integrazione;
10. Avvocati presenti nel dipartimento legale;
11. Non avvocati presenti nel dipartimento legale;
12. Competenze legali;
13. Spesa legale;
14. Attività puramente legali;
15. Attività non puramente legali;
16. Fornitori;
17. Analisi delle fatture;
18. Soddisfazione;
19. Aspettative;
20. Automazione;
21. Tecnologia disponibile;
22. Dati;
23. Reporting;
24. Formazione;
25. Knowledge management;
26. Knowledge management specifico;
27. Allineamento del rischio;
28. Propensione al rischio.

Il valore degli avvocati all'interno dell'azienda non consiste nel fornire gli input di un processo, ma nell'interpretare correttamente gli output, identificando esattamente l'anomalia legale di un sistema e fornendo consigli di alta qualità strategica. Comprendere e misurare questo enorme valore è una sfida ancora in corso che necessita di metodo, tecnologia, ma anche e soprattutto di un cambio di paradigma da parte degli avvocati, che sono chiamati a far emergere l'unicità della propria esperienza, conoscenza del settore e competenza. In questo senso, è fondamentale contribuire ad alimentare questo dibattito per catturare, aumentare e dimostrare il valore creato dai servizi svolti dal dipartimento legale. Ovviamente l'approccio ai KPI e alla tecnologia da implementare nel dipartimento legale dovrà essere sartoriale, strutturato e gestito: la pluralità dei legal tech tool presenti sul mercato e la complessità delle metriche rendono infatti la misurazione un'operazione articolata, da adattare alla singola organizzazione, ai diversi obiettivi perseguiti e alle particolari esigenze interne. Il Legal Management accompagna i General Counsel in questo viaggio di misurazione, fornendo il giusto supporto per affrontare tutte le nuove sfide legali.

Perché non esiste il dipartimento legale perfetto in assoluto, ma esiste sicuramente il dipartimento legale perfetto per l'organizzazione in cui opera.

TECNOLOGIE XDR E CONTESTI AZIENDALI: COME ADOTTARE UN APPROCCIO FORENSE E MIGLIORARE LA SECURITY POSTURE DELLA PROPRIA ORGANIZZAZIONE

Alessandro Di Carlo e Leonardo Summa, Certego

Nell'attuale scenario della sicurezza informatica, l'adozione delle tecnologie XDR (Extended Detection and Response) emerge come un'innovazione di fondamentale importanza per elevare il livello di protezione delle organizzazioni. Questa evoluzione assume particolare rilevanza in un contesto in cui le minacce informatiche si fanno sempre più complesse e insidiose, mettendo a rischio i dati sensibili, la reputazione e la continuità operativa delle aziende.

Le sfide da affrontare sono molteplici e necessitano di importanti risorse economiche e umane da dedicare nella mitigazione degli scenari di rischio presenti. L'eterogeneità di ogni azienda, in termini di business critici, di infrastrutture informatiche, di dimensionamento e struttura organizzativa, impone il ricorso a servizi sartoriali che consentano di poter modellare l'adozione di processi, misure tecnico-organizzative e soluzioni tecnologiche alle peculiarità della propria realtà.

L'adozione di un approccio forense nella gestione della sicurezza informatica aziendale può rappresentare una valida alternativa alle metodiche tradizionali, offrendo una maggiore efficacia in termini di rilevamento e risposta ad incidenti di sicurezza, riducendo l'impatto aziendale di eventuali attività malevole e i costi di ripristino correlati.

Tipicamente le attività di Digital Forensics e quelle di Incident Response (DFIR) presentano, al contempo, aree di sovrapposizione e differenze significative, rispondendo ad esigenze ontologicamente differenti. Le attività di risposta e gestione di un incidente di

sicurezza si caratterizzano per la loro criticità e tempestività, al fine di gestire l'incidente e contenere eventuali danni ulteriori; di contro, le attività di raccolta, conservazione e analisi degli artefatti correlati ad un incidente di sicurezza, finalizzate ad un futuro utilizzo in ambito giudiziario, si contraddistinguono per essere spesso eseguite post-mortem con l'obiettivo di ricostruire quanto già accaduto.

Il processo di gestione delle evidenze digitali si articola in diverse fasi topiche: l'identificazione e l'acquisizione degli artefatti di interesse; la raccolta e conservazione degli artefatti acquisiti; infine, l'analisi e la presentazione dei riscontri ottenuti.

Pragmaticamente, ciascuna delle fasi descritte ha un impatto specifico in termini di tempistiche e competenze necessarie per essere eseguite, motivo per il quale potrebbero non essere la soluzione più efficace da adottare per la gestione di incidenti di sicurezza.

«L'adozione di un approccio forense nella gestione della sicurezza informatica aziendale può rappresentare una valida alternativa alle metodiche tradizionali, offrendo una maggiore efficacia in termini di rilevamento e risposta ad incidenti di sicurezza, riducendo l'impatto aziendale di eventuali attività malevole e i costi di ripristino correlati.»

In caso di incidenti di sicurezza, superata la concitata fase di Incident Response, l'esigenza primaria per ogni organizzazione è raccogliere tutti gli artefatti necessari per approfondire l'analisi di quanto accaduto e valutare eventuali azioni giudiziarie da intraprendere.

Sebbene l'approccio tradizionale della Digital Forensics mantenga alcuni benefici significativi, come la possibilità di esaminare una copia forense completa dei sistemi compromessi e condurre indagini specifiche (es. retro-hunting, supertimeline, etc.) in funzione della tipologia di incidente subito, permangono alcuni limiti strutturali che meritano di essere superati.

L'adozione di modelli di risposta innovativi e fortemente adattivi, come il ricorso alle tecnologie XDR e ai servizi di Managed Detection & Response (MDR), consente di

fronteggiare con maggiore efficacia gli attacchi e le minacce più evolute, coniugando le esigenze di raccolta di tutti gli artefatti rilevanti secondo metodologie forensi.

Spesso, nella gestione della postura di sicurezza aziendale, la bussola per orientarsi viene ritrovata nella normativa europea e nazionale (NIS, GDPR, DORA, AGID), nelle certificazioni di processi aziendali (standard ISO, NIST) e nella conformità a linee guida di settore (PSD, ACN, PNSC).

La complessità delle problematiche sollevate dalla gestione della sicurezza informatica e dalla conformità con il quadro normativo vigente viene tradizionalmente risolta con il ricorso a servizi consulenziali e/o strategie di outsourcing nei diversi settori aziendali coinvolti.

La proposta di adottare le tecnologie XDR per migliorare la security posture aziendale e adottare un approccio forense by default rappresenta una soluzione alternativa per la gestione del rischio informatico aziendale e per governare le imprevedibili sfide del quotidiano di ogni organizzazione.

I benefici che derivano dall'implementazione di tali tecnologie sono molteplici e di significativa importanza sotto differenti profili. In primis, l'applicazione di tecnologie XDR che raccolgono e analizzano in near real-time i dati telemetrici generati dai diversi sistemi presenti (network, client, server, cloud) consente di avere una visibilità maggiore sul perimetro aziendale monitorato e di ridurre i tempi di rilevamento (MTTD) e risposta (MTTR) in caso di eventuali attacchi.

Inoltre, non bisogna dimenticare che tali tecnologie, grazie alla loro capacità di catturare telemetria proveniente dai sistemi su cui risultano installate, possono essere utilizzate anche per rispondere a "semplici" quesiti tipici di qualsiasi indagine forense; sia essa riferita alla sottrazione di know-how aziendale da parte di un dipendente infedele, che alla copia non autorizzata di codice sorgente facente parte della proprietà intellettuale dell'azienda stessa.

Oltre l'impatto significativo sul processo di investigazione e risposta alle minacce, i benefici delle soluzioni XDR si concretizzano in termini di scalabilità nell'adozione della soluzione ed efficienza economica nella riduzione del rischio di compromettere la continuità operativa in caso di incidenti.

Anche in questo caso, la tecnologia XDR svolge egregiamente la sua funzione in quanto,

grazie alla possibilità di utilizzare le cosiddette funzioni di "Live Response", ovverosia quelle caratteristiche che ci consentono di interagire direttamente sulla macchina target, risulterebbe estremamente facile creare una copia forense integrale del sistema comodamente da remoto.

Tuttavia si devono considerare alcuni limiti insiti nell'adozione di tali tecnologie, come la necessità delle adeguate competenze in grado di analizzare il dato telemetrico raccolto, la compatibilità di adozione in infrastrutture datate, la presenza crescente di numero di falsi positivi in architetture con una maggiore complessità e la riduzione delle capacità di condurre attività di retro-hunting.

«La proposta di adottare le tecnologie XDR per migliorare la security posture aziendale e adottare un approccio forense by default rappresenta una soluzione alternativa per la gestione del rischio informatico aziendale e per governare le imprevedibili sfide del quotidiano di ogni organizzazione.»

A ciò si deve aggiungere un tassello fondamentale nella costruzione di un modello di difesa adattivo ed efficace, rappresentato dalla Threat Intelligence e dalle capacità di azionare le informazioni raccolte, relative ad IoC e BIoC costruiti dallo studio delle TTPs (Tattiche, Tecniche e Procedure), nel proprio contesto aziendale.

Infine, l'implementazione del modello descritto realizza un beneficio indiretto che consiste nella creazione di un flusso di monitoraggio continuo basato sulla raccolta dei dati telemetrici, secondo un approccio forense, l'attivazione tempestiva di attività di contenimento e risposta in caso di incidenti di sicurezza e l'arricchimento delle capacità di rilevamento, con l'integrazione di fonti di Threat Intelligence esterne e interne costruite sulla base degli eventi rilevati all'interno del perimetro monitorato.

In conclusione, le tecnologie XDR offrono una straordinaria opportunità per migliorare la security posture delle organizzazioni e per adottare un approccio forense by default, ottenendo molteplici benefici in un'unica soluzione in grado di ridurre i tempi di gestione e analisi degli incidenti di sicurezza, in maniera scalabile e integrabile con servizi di Threat Intelligence.

L’IA SOSTITUIRÀ GLI AVVOCATI E ALTRE STORIE FANTASTICHE

Debora Elia, Innextart

Scommetto che tutti, almeno una volta, avete letto o sentito la frase: “L’intelligenza artificiale sostituirà gli avvocati!”. Scommetto anche che, se siete dei giuristi, colui che vi diceva questa frase aveva stampato in faccia un sorrisetto vagamente provocatorio. Non mi fermo e rilancio: avete mai riflettuto su chi sia l’autore di queste discussioni infinite su social network vari? Chi è il collega o l’amico che prova a convincervi del fatto che presto, prestissimo, l’utilizzo dell’IA renderebbe quasi superflue figure come quelle dell’avvocato, del magistrato e del notaio?

L’ultima scommessa: l’autore, il collega o l’amico non sono dei giuristi.

Non per qualche astrusa motivazione che voglia “elevare” la categoria, ma per il semplice fatto che molti degli argomenti che ispirano questi articoli, per il diritto e i suoi operatori semplicemente non sono rilevanti o partono da premesse fallaci.

I LARGE LANGUAGE MODELS

Una delle premesse fallaci riguarda i Large Language Models, ma è necessario prima fare chiarezza su cosa essi siano.

I modelli linguistici di grandi dimensioni o LLM rientrano in quella che viene definita come “Intelligenza artificiale debole”, in quanto è progettata per eseguire compiti specifici e limitati, come la comprensione e la generazione di testo in linguaggio naturale in risposta a input umani.

I LLM si basano su algoritmi di deep learning e vengono addestrati su un elevato numero di set di dati, utilizzano una rete neurale artificiale, che è un sistema computazionale ispirato al funzionamento del cervello umano[1] per imparare a prevedere la parola successiva in una sequenza, in base al contesto fornito dalla parola precedente.

Un noto esempio di LLM è GPT-4, sviluppato da OpenAI.

Ecco qui la premessa fallace: pensare che un generatore di testo possa sostituirsi ad una figura professionale vuol dire presumere che questa figura si occupi esclusivamente di generare testo[2]. L'IA non capisce, non conosce regole grammaticali, non usa il linguaggio per argomentare, persuadere o difendere, non ha una strategia né uno scopo, aggrega parole su base probabilistica.

È vero che agli avvocati piace scrivere infiniti muri di testo, ma che facciano solo questo mi sembra un tantino riduttivo.

L'HYPE

Nel 2023 sono state diverse le notizie sensazionali, giunte in special modo dagli Stati Uniti: dall'avvocato "robot" della startup DoNotPay a GPT-4 che supera lo Universal Bar Exam.

Il clamore (e rumore) arriva, a mio avviso, per l'hype generato da ChatGPT, il famosissimo chatbot di OpenAI.

In realtà strumenti di IA vengono già utilizzati dai legali, è pacifico ad esempio l'utilizzo dei software di contract lifecycle management, quasi tutti dotati di applicazioni basate sull'AI, pensiamo a DocuSign CLM, Agiloft e così via.

Qualcuno ha definito l'IA come "il tirocinante non pagato che non dorme mai", sarà meno di impatto rispetto all'avvocato robot, ma forse più realistico.

1 *Cos'è in AI il LLM: introduzione al Large Language Model, disponibile a quest'indirizzo:* https://www.punto-informatico.it/cose-in-ai-il-llm-introduzione-al-large-language-model/

2 *Eliza Mik, Will LLMs replace lawyers?, luglio 2023, disponibile a quest'indirizzo:* https://elizamik.medium.com/llms-will-not-replace-lawyers-d491e7c655ca

I RISCHI

Cito il caso che vede protagonisti gli avvocati Steven Schwartz e Peter LoDuca per introdurre uno dei problemi dell'IA: le allucinazioni.

Il caso in esame riguarda un uomo che cita in giudizio la compagnia aerea Avianca, sostenendo di essere rimasto ferito durante un volo. La compagnia aerea ha chiesto al giudice di archiviare la causa per decorso dei termini di prescrizione, gli avvocati dell'uomo hanno risposto presentando al giudice una memoria di dieci pagine, citando diversi precedenti giudiziari a sostegno della loro tesi.

È stato chiesto agli avvocati di fornirne delle copie dei precedenti: si è scoperto che i casi non erano reali. Schwartz ha confessato di aver utilizzato ChatGPT, poiché pensava che fosse "un super motore di ricerca"[3]. Lui ed il suo collega sono stati poi multati con una sanzione di cinquemila dollari[4].

Le allucinazioni sono uno dei problemi dei LLMs, spesso infatti questi modelli generano testo perfettamente logico e credibile ma completamente falso, inventato.

Numerosi poi i rischi sotto il profilo della sicurezza, della protezione dei dati personali, della responsabilità, del diritto d'autore o del copyright.L'addestramento dei sistemi di IA necessita di enormi quantità di dati, fra quelli interessati dal processo di estrazione, chiamato Text and Data Mining (TDM), ci potrebbero essere delle opere creative tutelate dalla disciplina del diritto d'autore o da un diritto connesso[5].

Anche se queste informazioni fossero liberamente accessibili online, ciò non significherebbe necessariamente che il proprietario dei dati abbia acconsentito alla loro divulgazione, né che i dati siano disponibili senza restrizioni o vincoli specifici di utilizzo o licenze[6].

Inoltre il web scraping, ossia il processo di estrazione automatizzata di informazioni

---

3 *The ChatGPT Lawyer Explains Himself, disponibile a quest'indirizzo: https://www.nytimes.com/2023/06/08/nyregion/lawyer-chatgpt-sanctions.html*

4 *New York, multa di 5mila dollari a due avvocati per aver citato casi legali falsi consigliati da ChatGPT, disponibile a quest'indirizzo: https://www.open.online/2023/06/23/usa-avvocati-multati-chatgpt/*

5 *Simone Aliprandi, L'autore artificiale, 2023, p. 73*

6 *Simone Aliprandi, ibidem*

da siti web o altre fonti di dati online, potrebbe costituire violazione dei termini d'uso della piattaforma analizzata.Un caso giurisprudenziale riguardante il problema dello scraping è quello che vede coinvolte Getty Images e Stability AI. A inizio 2023, Getty Images ha intentato una causa negli Stati Uniti contro Stability AI, sostenendo che quest'ultima avesse violato i propri diritti d'autore, copiando senza permesso più di 12 milioni di fotografie, correlate da didascalie e metadati, per addestrare il proprio sistema di Stable Diffusion. Getty ha chiesto un risarcimento danni fino a 150.000 dollari per opera violata, portando potenzialmente l'entità del risarcimento richiesto a 1,8 miliardi di miliardi di dollari[7]. Getty Images ha poi chiesto alla High Court of Justice di Londra un'ingiunzione per impedire alla società di intelligenza artificiale di vendere il suo sistema di generazione di immagini AI in Gran Bretagna, secondo quanto emerso dai documenti giudiziari[8].

«L'addestramento dei sistemi di IA necessita di enormi quantità di dati, fra quelli interessati dal processo di estrazione, chiamato Text and Data Mining (TDM), ci potrebbero essere delle opere creative tutelate dalla disciplina del diritto d'autore o da un diritto connesso.»

IL TEMPO DELLA CONSAPEVOLEZZA

Senza dubbio le potenzialità dell'IA sono impressionanti e avranno un grosso impatto sulle professioni legali ma se numerose sono le opportunità ed i benefici, altrettanto numerosi sono i rischi.Se da un lato il lavoro cambierà ed alcune attività saranno automatizzate o eliminate, dall'altro l'insorgenza di nuove problematiche porterà nuove opportunità ed una maggiore richiesta di esperti legal tech.

È passato il tempo dell'entusiasmo, è arrivato il tempo del dibattito.

---

7 *Photo giant Getty took a leading AI image-maker to court. Now it's also embracing the technology, disponibile a quest'indirizzo:* https://apnews.com/article/getty-images-artificial-intelligence-ai-image-generator-stable-diffusion-a98eeaaeb2bf13c5e8874ceb6a8ce196

8 *Getty asks London court to stop UK sales of Stability AI system, disponibile a quest'indirizzo:* https://www.reuters.com/technology/getty-asks-london-court-stop-uk-sales-stability-ai-system-2023-06-01/

PROFILI DI RESPONSABILITÀ ALLA LUCE DELLA PROPOSTA DI REGOLAMENTO EUROPEO SULL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Silvia Enrico e Alessandro Lardo, 4Legal

L'utilizzo dell'Intelligenza Artificiale (AI) è al centro di un accesissimo dibattito sul quale si sono pronunciati una moltitudine di esperti del settore e non. Comunque la si pensi in proposito, resta il fatto che l'AI è un fenomeno con cui doversi confrontare su più livelli; dai settori di possibile impiego ed evoluzione, agli aspetti normativi e di responsabilità giuridica coinvolte. Infatti, in questo dibattito anche Bill Gates ha espresso il suo punto di vista, mettendo in guardia Google ed Amazon, affermando che l'AI cambierà le abitudini dei consumatori. Non siamo davanti ad un responso fumoso ma siamo di fronte ad un monito ben preciso indirizzato a due Big Company del panorama tech mondiale. Perché proprio Google ed Amazon, è presto detto, basta osservare l'utilizzo più frequente che viene fatto dell'AI: quello della profilazione, della selezione di prodotti ed indirizzamento delle scelte dei consumatori.

Così l'AI ha superato anche il Machine Learning, che solo qualche anno fa sembrava uno strumento avveniristico. Il Machine Learning, infatti, si limita a simulare modelli di comportamento e decidere quanto più in linea possibile con i dati aggregati ricevuti dall'utenza. Il modello del data analysis utilizzato dal Machine Learning, per quanto futuristico, è meno impressionante della tecnologia AI, che supera ogni barriera tecnologica ed arriva a simulare il pensiero umano.

Proprio per la molteplicità di impieghi in cui l'AI può essere utilizzata e per la peculiare dote di riuscire a simulare i comportamenti ed i pensieri umani, la Commissione Europea, il 14 giugno scorso, ha sottoposto all'attenzione del Parlamento Europeo una proposta di

regolamento per l'utilizzo della stessa, ponendo limiti ben definiti.

La proposta da parte della Commissione mira ad assicurare un utilizzo dell'AI che sia sicuro, trasparente, tracciabile, non discriminatorio e rispettoso dell'ambiente. Per tale ragione la Commissione Europea vuole identificare dei livelli di rischio ben definiti, e sulla base di tali rischi porre dei limiti all'utilizzo degli strumenti di Intelligenza Artificiale.

Nella bozza di regolamento, per l'utilizzo dei sistemi di AI, vengono identificati tre livelli di rischio.

Vengono considerati "rischi inaccettabili" che costituiscono una minaccia per le persone, quelli connessi alla (i) manipolazione comportamentale cognitiva di persone o gruppi vulnerabili, (ii) classificazione delle persone in base al comportamento, al livello socioeconomico ed alle caratteristiche personali, (iii) utilizzo di sistemi di identificazione biometrica in tempo reale e a distanza. Per tali scopi, la Commissione Europea nella bozza di regolamento, intende vietare l'utilizzo di strumenti d'Intelligenza Artificiale.

Vengono considerati invece a "rischio alto" tutti quegli impieghi in cui l'AI può influire negativamente sulla sicurezza o sui diritti fondamentali delle persone. A tal riguardo la Commissione ha diviso gli impieghi considerati a "rischio alto" in due sottocategorie:

1. quando l'AI viene integrata a tutti quegli strumenti che sono sottoposti al controllo della Direttiva EU2001/95/CE sulla sicurezza dei prodotti (si pensi a smartphone, automobili, strumenti domotici in generale che integrano funzioni di Intelligenza Artificiale);
2. più in generale, quando l'AI viene utilizzata in tutti quei processi di identificazione e categorizzazione biometrica, gestione e funzionamento di infrastrutture critiche, istruzione e la formazione professionale, selezione ed occupazione, gestione dei lavoratori, accesso e fruizione di servizi privati e pubblici essenziali, ausilio alle forze dell'ordine, gestione dei flussi migratori e controllo delle frontiere, assistenza nell'interpretazione della legge.

Per tutti questi impieghi la Commissione ha previsto di affiancare ai sistemi di Intelligenza Artificiale il monitoraggio di un essere umano, che sorvegli costantemente il lavoro dell'AI allo scopo di valutarne i risultati e prevenire eventuali errori ed interpretazioni

dello strumento tecnologico.

In ultimo, nella proposta di regolamento, vengono presi in considerazione strumenti più semplici, definiti a "rischio limitato", come l'AI generativa (ad esempio ChatGPT), per le quali la Commissione Europea vorrebbe prevedere che vengano rispettati i requisiti minimi di trasparenza ed informazione, ogniqualvolta l'AI generi o manipoli informazioni nel processo di interazione con l'utenza.

Gli aspetti più interessanti sui quali riflettere sono sicuramente quelli legati ai profili di responsabilità legati all'utilizzo dell'AI su larga scala ed a fini commerciali ed imprenditoriali.

«Proprio per la molteplicità di impieghi in cui l'AI può essere utilizzata e per la peculiare dote di riuscire a simulare i comportamenti ed i pensieri umani, la Commissione Europea, il 14 giugno scorso, ha sottoposto all'attenzione del Parlamento Europeo una proposta di regolamento per l'utilizzo della stessa, ponendo limiti ben definiti.»

Per attività considerate dalla proposta di regolamento a "rischio alto" (e pertanto soggetto al monitoraggio dell'essere umano), sarà necessario stabilire qual è il confine fra la responsabilità del soggetto supervisore delle attività dell'Intelligenza Artificiale e quello della società che sviluppa e fornisce gli strumenti che utilizzano l'AI, al fine di determinare il danno e quantificare la responsabilità. Ad esempio, in caso di malfunzionamento di un impianto nel quale alcuni processi produttivi sono delegati a software di Intelligenza Artificiale, dove finisce la responsabilità del supervisore e dove inizia quella della software-house che ha sviluppato lo strumento di monitoraggio basato su tecnologie di Intelligenza Artificiale?

Se invece volessimo prospettare una serie di casi che possono verificarsi su una scala molto più ampia, di fronte ad uno strumento di Intelligenza Artificiale generativa a supporto di un e-commerce o di un sito di comparazione dei prodotti, qualora il prodotto dovesse mancare delle qualità promesse, o addirittura dovessimo trovarci davanti ad un caso di aliud pro alio, in che termini il gestore del sito di e-commerce/di comparazione

potrà rivalersi sulla software-house che sviluppa il sistema di comparazione? Oppure in che termini il consumatore con capacità di giudizio e di scelta – informato dell'utilizzo di un sistema automatico di selezione e comparazione – potrà far valere i propri diritti relativamente ad eventuali omissioni ingannevoli (ex art. 22 codice del consumo)? O addirittura, in ultimo, in che termini si profilerebbe un concorso in colpa del danneggiato ex art. 1227 C.c. nel caso in cui si dimostrasse che l'utente era assolutamente consapevole dell'utilizzo di sistemi di AI e dell'eventuale margine di errore, ed aveva tutti gli strumenti necessari per poter valutare l'aderenza del prodotto alle proprie esigenze?

Come sempre, le nuove tecnologie portano il diritto ad inseguire abitudini già spesso consolidate nella prassi. La nota positiva che traspare dalla tempestività con la quale la Commissione Europea ha voluto agire, è che in questa circostanza sembrerebbe che il diritto non seguirà affannosamente i cambiamenti della tecnologia ma si muoverà plasticamente insieme a questo cambiamento, continuando a garantire una piena tutela dei diritti di ogni membro della comunità europea.

RANSOMWARE:
PREVENZIONE E REAZIONE

Giuseppe Fornari e Nicolò Biligotti, Fornari e Associati

Il ransomware è una specifica, e particolarmente insidiosa, tipologia di malware (malicious software): esso, oltre a criptare (crypto ransomware) o comunque a rendere inaccessibili (locker ransomware) i file presenti nei dispositivi o nelle reti informatiche aziendali, trasmette alla vittima una richiesta di riscatto il cui pagamento diviene strumentale al recupero dell'accesso ai dati aziendali, nonché, molto spesso, alla tutela della loro riservatezza nei confronti di terzi. Omettere il pagamento del riscatto, nella pressoché totalità dei casi richiesto in bitcoin o altra valuta virtuale, significa incorrere in pesanti conseguenze sul piano economico e giuridico: i dati informatici, una risorsa cruciale per la produttività aziendale, potrebbero emergerne definitivamente compromessi, e la loro divulgazione a terzi sfociare in costi connessi alla perdita di know-how esclusivo, a danni reputazionali e alle ingenti sanzioni previste dalla normativa GDPR.

Mentre il fenomeno è in netta diffusione – in poco più di un anno (maggio 2021 - giugno 2022) circa 10 terabyte di dati al mese sono stati coinvolti in ransomware attacks – non è ad oggi stata sviluppata una strategia univoca di prevenzione e reazione fondata su best practices consolidate. Senz'altro auspicabile è la creazione di un legal framework che – tramite interventi normativi, finanziamento di fondi per la fase di attack recovery e modelli di collaborazione ai fini di information intelligence – persegua alcuni obiettivi essenziali: (i) lo sviluppo di una coordinata strategia di deterrenza; (ii) l'annichilimento del ransomware business model; (iii) la delineazione di modelli organizzativi orientati

alla prevenzione e reazione.

Nell'arretratezza del quadro normativo, emerge l'evidenza empirica: un ransomware attack è un evento dal grande impatto economico-giuridico, la cui prevenzione richiede un approccio sistematico e la cui strategia di reazione richiede delicate valutazioni da compiersi in un contesto convulso e condizionato dall'urgenza.

Per quanto attiene all'efficacia dell'attività di prevenzione, essa si pone in rapporto di proporzionalità diretta con i generali presidi in materia cybersecurity, così come delineati dall'attuale normativa vigente: sul punto, vengono in particolare rilievo le misure tecnico-organizzative imposte dall'art. 21 Direttiva NIS 2 e dall'art. 32 GDPR. È significativo notare come anche i più basilari presidi di igiene informatica possano drasticamente ridurre le probabilità di un ransomware attack e, comunque, i danni da esso attesi.

«Mentre il fenomeno è in netta diffusione – in poco più di un anno (maggio 2021 - giugno 2022) circa 10 terabyte di dati al mese sono stati coinvolti in ransomware attacks – non è ad oggi stata sviluppata una strategia univoca di prevenzione e reazione fondata su best practices consolidate.»

A titolo di esempio, nell'ampio catalogo dei richiamati presidi: aggiornamento dei software e degli anti-virus; minimizzazione delle licenze di accesso e dei privilegi di amministratore; aggiornamento delle password di accesso e autenticazione multifattoriale; sicurezza fisica e limitazione delle funzionalità dei devices aziendali (e.g. pre-approvazione all'installazione di app e software); frequente off-line backup secondo lo schema 3-2-1 (3 copie locali, 2 diversi supporti di memorizzazione e 1 copia fuori sede); crittografia dei dati; formazione delle risorse umane (e.g. scrupoloso controllo dei domini e-mail in logica anti-phishing); e così via.

Un solido apparato cybersecurity è cruciale nel dissuadere gli hackers dal perpetrare l'attacco ransomware: in ultima istanza, ciò è vero nella fase di social engineering che spesso precede l'attacco informatico, allorquando i criminali sono già penetrati in qualche misura nella rete aziendale e ne monitorano in via occulta l'organizzazione

al fine di identificare le vulnerabilità di sistema e valutare le chances di successo dell'attacco informatico.

Venendo alla strategia di reazione ad un attacco ransomware, essa richiede il dispiego di una task force composta da professionisti dalle competenze differenziate, in grado di intervenire in modo rapido e coerente (IRT, Incident Response Team). In tale contesto:

- Spetta ad esperti di sicurezza informatica (Forensic Analysts) il compito di identificare i dati interessati dall'attacco, isolare i sistemi infetti e, ove possibile, ripristinare i file. Pure in assenza di un off-line backup da cui attingere, risulta essenziale la verifica dell'esistenza di possibili copie dei dati non affette dall'attacco informatico, nonché l'identificazione dello specifico ransomware da cui il sistema è stato colpito, al fine di valutare la disponibilità di una chiave di decrittazione che consenta il recupero dei dati pure nell'inadempimento al pagamento del riscatto;
- Un avvocato penalista, esperto in cybercrime, i cui compiti sono molteplici: qualificare i fatti occorsi e valutare il deposito di un atto di esposto alla Procura della Repubblica; valutare e minimizzare eventuali responsabilità penali della vittima, persona fisica e giuridica che si determini al pagamento del riscatto (e.g. false comunicazioni sociali, riciclaggio, reati tributari, responsabilità amministrativa da reato ex d.lgs. n. 231/2001, aggiramento di sanzioni UE nei confronti dello Stato russo); elaborare, in sinergia con i componenti dell'IRT, la matrice costi-benefici che illustri, in chiave economica, pro e contro delle due alternative disponibili (pagare o non pagare il riscatto); valutare, sulla base delle serie storiche disponibili, la possibilità che i dati non vengano de-criptati pure in caso di pagamento del riscatto, nonché la possibilità che ad una prima richiesta di riscatto volta alla de-criptazione dei dati ne faccia seguito una seconda finalizzata ad evitare la diffusione degli stessi (ove esfiltrati dai criminali informatici); coadiuvare i blockchain specialists nella eventuale negoziazione con i criminali nell'eventuale corresponsione del riscatto in valuta virtuale e, per quanto possibile, nel monitoraggio on-chain delle somme corrisposte;
- Data Protection Officer e Data Protection Specialist rivestono infine un ruolo fondamentale nell'assicurare la compliance con la normativa privacy e, in tale ottica, nel valutare e gestire gli obblighi di breach notification nei confronti dell'Autorità Garante e dei data subjects. Si noti: non ogni ransomware attack

comporta obblighi di notifica all'Autorità Garante e ai data subjects; il primo obbligo di notifica (nei confronti dell'Autorità) si attiva in presenza di un rischio per i diritti e le libertà fondamentali delle persone fisiche interessate, mentre il secondo obbligo di notifica (nei confronti dei data subjects) viene a sussistere, fatte salve alcune deroghe, soltanto in presenza di un alto rischio per i loro diritti e libertà fondamentali. Siffatte valutazioni, essenziali ai fini della minimizzazione dell'impatto del ransomware attack sulla vittima, nonché da compiersi alla luce delle misure tecnico organizzative implementate pre e post attacco informatico, lasciano tuttavia inalterato l'obbligo di conservazione delle informazioni inerenti all'evento e gli obblighi di notifica nei confronti dell'Agenzia per la Cybersicurezza Nazionale previsti dalla Direttiva NIS2 (ove applicabile).

L'ultimo sforzo del team è sempre quello di adiuvare la vittima a reagire in ottica lesson learned: si procede all'identificazione delle vulnerabilità del sistema IT che hanno reso possibile l'attacco ransomware e vi si pone rimedio.

L'ARMONIA TRA TECNOLOGIA E UMANITÀ NELLA GESTIONE DEL PATRIMONIO. UN'ANALISI CRITICA DEI RUOLI DI ROBO-ADVISOR E CONSULENTI FINANZIARI

Alessio Grazia, Allianz Bank Financial Advisors

Lo sviluppo crescente di strumenti digitali finanziari sta comportando un ricorso alla tecnologia sempre più frequente nella gestione dei patrimoni.

L'emergere, in particolare, dei robo-advisor basati sull'intelligenza artificiale ha rivoluzionato l'approccio alla gestione degli investimenti, offrendo efficienza e accessibilità senza precedenti. L'automazione finanziaria è in espansione: tuttavia, la sicurezza finanziaria e il benessere degli investitori dipendono dal delicato equilibrio tra la precisione algoritmica e l'empatia umana.

Sia il ricorso alle funzionalità dei robo-advisor che all'esperienza dei consulenti finanziari in carne e ossa presentano dei vantaggi. Da un lato, rivisitare i processi utilizzando tecnologie digitali, con l'obiettivo di renderli più efficienti, potenziando in quantità e qualità la raccolta dei dati, è un passaggio necessario. Il mondo attuale dimostra che si tratta di un cambiamento di prospettiva ormai irreversibile. Allo stesso tempo, però, affidarsi esclusivamente a processi automatizzati nella pianificazione finanziaria non è una scelta esente da rischi e da possibili danni. Perché immaginare una gestione ottimale del patrimonio senza basarla sulla comprensione individuale, sul supporto emotivo e sulla risposta personalizzata, è, ragionevolmente, impossibile.

Di fatto, l'armonia tra tecnologia e presenza umana rappresenta il futuro della gestione del patrimonio, poiché garantisce una consulenza finanziaria completa, consapevole ed efficace per gli investitori di oggi e di domani.

DOVE IL SILICIO NON PUÒ ARRIVARE

I robo-advisor hanno dimostrato di essere strumenti interessanti per l'abbattimento dei costi del servizio. L'automazione, del resto, in questo come in ogni altro settore, rende più efficaci i processi: quando questi vengono migliorati, diventano meno onerosi.

Nella gestione del patrimonio, però, è fondamentale riconoscere le situazioni in cui il solo approccio automatizzato delle piattaforme di servizi fintech può risultare inadeguato.

MANCANZA DI COMPRENSIONE DELLE ESIGENZE INDIVIDUALI

Uno dei principali ostacoli per i robo-advisor è la mancanza di capacità di comprensione delle esigenze finanziarie individuali. Questi algoritmi, pur basandosi su dati forniti dagli utenti, spesso non riescono a considerare le sfumature date dalle attitudini personali, i desideri e gli obiettivi unici di ogni investitore. Ciò può portare a strategie di investimento che non tengono pienamente conto delle necessità specifiche.

«Di fatto, l'armonia tra tecnologia e presenza umana rappresenta il futuro della gestione del patrimonio, poiché garantisce una consulenza finanziaria completa, consapevole ed efficace per gli investitori di oggi e di domani.»

I questionari di profilazione MIFID non tengono, infatti, in considerazione le evoluzioni che possono avere le condizioni di vita degli investitori. Pur potendo programmare un robo-advisor per "interrogare" l'investitore all'inizio del suo percorso, così da profilarlo in uno dei vari segmenti, non sempre quelle risposte resteranno attuali nel corso del tempo. Anzi. Una nascita, una morte, un cambio di lavoro o di residenza impattano negli orizzonti – e quindi negli obiettivi – dei clienti. Difficilmente, ad oggi, un sistema automatico potrà cogliere certe variazioni nel tempo, che solitamente vengono sviscerate da domande umane, precise, anche in risposta a racconti spontanei. Questi, per i clienti, possono sembrare soltanto sfoghi o confessioni ma in realtà, per il professionista, rappresentano il cuore del lavoro.

ASSENZA DI SUPPORTO EMOTIVO

Gli investimenti sono spesso caratterizzati da periodi di volatilità del mercato e decisioni finanziarie stressanti. In queste situazioni, l'assenza di un apporto umano può essere problematica. I robo-advisor non possono fornire il supporto emotivo e la rassicurazione che un consulente finanziario – umano – può offrire durante i momenti difficili, aiutando gli investitori a evitare decisioni guidate dalle emozioni. Prendiamo ad esempio prolungati periodi sott'acqua (ossia dove il valore del portafoglio risulti inferiore al conferito). Lo stress si accumula, e va gestito: un robo-advisor non è programmato per lo stress, ma per la matematica.

INADEGUATEZZA NELLE SITUAZIONI COMPLESSE

Le situazioni finanziarie possono diventare complesse e intricate, specialmente per coloro che hanno esigenze finanziarie più articolate, come la pianificazione fiscale, la gestione della successione aziendale o la creazione di un portafoglio per obiettivi finanziari particolari. In queste circostanze, la capacità dei robo-advisor nel fornire consulenza dettagliata e strategie su misura può rivelarsi limitata. Per quanto la maggior parte delle norme che si devono seguire negli esempi citati sia di "facile upload", il servizio è attualmente rivolto all'ottimizzazione del portafoglio. Di conseguenza, mancherà la visione complessiva del patrimonio relegando la funzionalità alla sola gestione del "dossier titoli".

RISCHI DELL'INVESTITORE IMPRONTATO ALL'AUTOMAZIONE

Per gli investitori inesperti, c'è il rischio di diventare dipendenti dall'automazione senza comprendere appieno le decisioni finanziarie prese. Un investitore che si affida esclusivamente a un robo-advisor potrebbe non avere una comprensione adeguata delle strategie di investimento o delle implicazioni fiscali delle sue azioni finanziarie, con un rischio maggiore di prendere decisioni dannose per il proprio patrimonio.

EDUCAZIONE FINANZIARIA ESSENZIALE

La gestione del patrimonio richiede una solida base di conoscenza finanziaria. Gli investitori impreparati possono trovarsi in difficoltà se non comprendono appieno i

principi finanziari di base e le conseguenze delle loro decisioni. Pertanto, è fondamentale che acquisiscano una buona educazione finanziaria prima di affidarsi ad un robo-advisor per la risoluzione di ogni loro questione patrimoniale.

LA CARNE NON È DEBOLE

Nel mondo della gestione del patrimonio, emergono spesso dibattiti sull'efficacia dei robo advisor rispetto alla consulenza finanziaria classica. Mentre l'automazione può portare efficienza e convenienza, è essenziale ricordare che "la carne" – cioè la presenza umana – gioca un ruolo insostituibile nella gestione del proprio capitale.

EMPATIA E COMPRENSIONE

Uno dei tratti distintivi dell'uomo è la sua capacità di empatia. Nel rapporto che si instaura fra un cliente ed un wealth manager, questo può comprendere le speranze, paure, e aspirazioni finanziarie del cliente su un livello profondo. La comprensione delle attitudini personali consente al professionista di adattare la strategia di investimento per fare in modo che rispecchi appieno gli obiettivi e le sfumature individuali dell'investitore. La comunicazione, infatti, non è un semplice scambio di domande e risposte tramite il quale possa essere deciso un profilo. Le reazioni emotive, il linguaggio non verbale e le parole non dette sono, spesso, più importanti di un elenco puntato.

SUPPORTO IN MOMENTI DIFFICILI

Il percorso di investimento, che si articola per tutta la vita, è una montagna russa di alti e bassi. Quando il mercato è turbolento o si devono prendere decisioni finanziarie importanti, una presenza confortante al fianco dell'investitore può fare la differenza. Il consulente non offre solo consigli razionali: la sua funzione è anche fornire supporto emotivo. A volte, un incoraggiamento o la classica spalla su cui piangere possono essere risolutivi in termini di fiducia e tranquillità. Del resto, a posteriori, sappiamo tutti che chi aveva il patrimonio investito prima della crisi di Lehman, se non avesse fatto niente, sarebbe ora molto più ricco. Pur avendo dovuto affrontare un brutto periodo.

PIANIFICAZIONE AVANZATA

La gestione del patrimonio spesso va oltre la semplice creazione di un portafoglio. Situazioni complesse come la pianificazione fiscale, la successione aziendale o la gestione di rischi legati all'eredità richiedono una consulenza esperta. Un professionista ha l'esperienza e le conoscenze per affrontare in modo articolato queste sfide e creare strategie personalizzate che tengano conto di ogni aspetto della situazione finanziaria mutevole di ogni persona.

L'ARTE DELLA COMUNICAZIONE NELL'EDUCAZIONE FINANZIARIA

La comunicazione è un aspetto fondamentale nella gestione del patrimonio. Un wealth manager è un esperto nella traduzione di termini complessi in un linguaggio accessibile. Questa abilità permette di rendere consapevoli gli investitori, aiutandoli a comprendere appieno le decisioni finanziarie e i loro impatti. Ogni scelta è dettata da un motivo, sia questo tattico o strategico. Non sempre, però, la motivazione è di facile comprensione: il consulente umano può svolgere un ruolo chiave nell'educare i clienti sui principi finanziari e sulla logica delle strategie di investimento. Il motivo è evidente: gli investitori correttamente informati, e che condividono la strategia, prendono decisioni finanziarie migliori.

FUSIONE UOMO-MACCHINA: PERCHÉ NO?

Nella continua evoluzione del settore della gestione del patrimonio, la previsione di una collaborazione sinergica tra consulenti finanziari e robo-advisor emerge come una prospettiva intrigante. Sebbene abbiano caratteristiche e competenze diverse, la "fusione tra uomo e macchina" può portare ad un servizio ancora più efficiente e personalizzato, senza dover rinunciare alla presenza umana essenziale.

AUTOMAZIONE DEI COMPITI RIPETITIVI

Uno dei modi in cui i robo-advisor possono assistere i consulenti finanziari è attraverso l'automazione di compiti ripetitivi e di routine. Questa soluzione consente ai consulenti di concentrarsi su attività di valore aggiunto come la consulenza personalizzata e la comprensione profonda delle esigenze dei clienti. Il tema appare futile, eppure non

lo è. I non addetti ai lavori possono chiedersi se in una professione di questo calibro esistano davvero compiti ripetitivi e di routine. La risposta è netta: più di quanto il cliente investitore non si aspetti.

ANALISI DEI DATI SU LARGA SCALA

I robo-advisor eccellono nell'analisi di dati su vasta scala e nella generazione di report dettagliati. Di questa capacità si possono avvalere i consulenti finanziari per monitorare e ottimizzare i portafogli dei clienti in tempo reale, garantendo una gestione più reattiva e basata su dati concreti. Il potere computazionale, ovvio e logico per un computer, è in grado di sfruttare la velocità di raccolta e gestione delle informazioni. Delegare questa attività ai servizi fintech consente al wealth manager di valorizzare il tempo dedicato al cliente.

«Per gli investitori inesperti, c'è il rischio di diventare dipendenti dall'automazione senza comprendere appieno le decisioni finanziarie prese. Un investitore che si affida esclusivamente a un robo-advisor potrebbe non avere una comprensione adeguata delle strategie di investimento o delle implicazioni fiscali delle sue azioni finanziarie, con un rischio maggiore di prendere decisioni dannose per il proprio patrimonio.»

CONSULENZA BASATA SU SCENARI

I robo-advisor possono essere programmati per simulare una serie di scenari finanziari, consentendo ai professionisti di fornire consulenza informata basata su proiezioni realistiche. Nell'ottica di riprodurre scenari passati il riferimento è ai "backtest", mentre in funzione prospettica ci si può avvalere di "simulazioni Monte Carlo" oppure si può ricorrere alle probabili evoluzioni del portafoglio tramite il "Cono di Ibbotson". Questo aiuta gli investitori a prendere decisioni ponderate in base ai loro obiettivi e alle condizioni del mercato.

SUPPORTO NELL'ANALISI DEI RISCHI

L'analisi dei rischi è una componente fondamentale della gestione del patrimonio. I robo advisor possono effettuare analisi di rischio dettagliate, aiutando i consulenti a identificare potenziali vulnerabilità nei portafogli dei clienti e a sviluppare strategie di mitigazione. Se il principio più conosciuto in ambito finanziario è la diversificazione, sarebbe in realtà molto più interessante soffermarsi sul concetto di decorrelazione, in modo da avere una fotografia esatta di quanto si è esposti nel proprio portafoglio a determinati eventi economici possibili in futuro.

RUOLO CHIAVE DEL CONSULENTE

È importante sottolineare che, nonostante l'assistenza dei robo-advisor, il consulente finanziario umano rimane il cuore del servizio. La sua presenza fornisce il supporto emotivo, la comprensione personale e la consulenza avanzata che l'IA non può replicare completamente. Inoltre, il professionista agisce come un guardiano del processo, garantendo che le decisioni finanziarie siano allineate agli obiettivi del cliente.

UNO SKIPPER ED UNA BARCA A VELA

Agendo come filtri automatizzati, i robo-advisor offrono vantaggi evidenti.

Allo stesso tempo, però, è importante riconoscere le situazioni in cui il silicio non può sostituire la saggezza umana. Infatti, il costante diluvio di informazioni tipico dell'era digitale porta con sé anche dati di scarsa qualità, sempre a portata di smartphone, ed è spesso fonte di confusione e non di educazione finanziaria.

Quindi gli investitori devono essere consapevoli delle limitazioni di tali strumenti e, in particolare per le decisioni finanziarie più complesse, confrontarsi con un consulente finanziario umano per ottenere una gestione del patrimonio completa, sicura e consapevole.

Il motivo per cui il professionista rimane insostituibile nel fornire un supporto personalizzato e un controllo sul processo è evidente: la presenza umana è connotata da empatia, comprensione, e competenza avanzata che l'automazione ad oggi non può replicare.

Nella ricerca della sicurezza finanziaria e del successo degli investimenti, infatti, serve sapere di non essere mai soli, perché alcuni momenti possono essere – e saranno – molto dolorosi se affrontati in solitudine.

Per questo, la fusione uomo-macchina nella gestione del patrimonio è una prospettiva promettente. I robo-advisor possono assistere i consulenti finanziari nell'automazione dei compiti, nell'analisi dei dati e nella simulazione di scenari. Si tratta di una cooperazione che può rendere il servizio fornito ai clienti ancora più personalizzato ed efficiente.

«Il percorso di investimento, che si articola per tutta la vita, è una montagna russa di alti e bassi. Quando il mercato è turbolento o si devono prendere decisioni finanziarie importanti, una presenza confortante al fianco dell'investitore può fare la differenza.»

La collaborazione fra umanità e intelligenza artificiale sarà, ed è tuttora, il modello ideale da sviluppare per far evolvere ulteriormente la professione nel nuovo millennio.

Dovrebbe essere ormai alle spalle la concezione di rivalità tra uomo e tecnologia: il pensiero deve tendere non verso quanto il professionista possa perdere, ma verso quanto possa dare.

Una barca a vela senza un buono skipper non regge il mare aperto. Un buono skipper, con una zattera, non regge il mare aperto. Un buono skipper con un'imbarcazione all'avanguardia può portare chiunque a destinazione. Anche quando il mare è agitato.

10 OSTACOLI ALL’INNOVAZIONE NEGLI STUDI LEGALI. UNA PROSPETTIVA ITALIANA

Marco Imperiale, Better Ipsum

Parlare di innovazione negli studi legali italiani tende ad evocare sentimenti contrastanti. Da un lato, e soprattutto dopo l'ascesa di ChatGPT e degli LL.M.s, si nota un progresso evidente in termini di trasformazione digitale e utilizzo di piattaforme tecnologiche, nonché un crescente interesse nel campo. Purtuttavia, è chiaro ai vari stakeholder che nel settore mancano cambiamenti strutturali per favorire un vero e proprio “cambio di passo”.

In questo articolo, esaminerò dieci fattori che, a mio vedere, ostacolano l'innovazione nello scenario legale italiano, in particolare con riguardo agli studi professionali. Mentre alcune barriere nascono da sfumature culturali, altre derivano da vincoli finanziari o da variabili completamente diverse. Prima di addentrarci ulteriormente nell’analisi, è fondamentale effettuare tre considerazioni:

- In primo luogo, il termine “innovazione” nel mondo legale è sfaccettato, passando dalla trasformazione digitale degli studi legali, all’efficientizzazione del sistema giudiziario, ai sistemi alternativi di risoluzione delle controversie;
- In secondo luogo, ogni discussione sugli impedimenti all'innovazione necessita di una chiara comprensione su cosa il concetto di innovazione realmente comprenda;
- In terzo luogo, un serio passaggio del sistema legale verso l'innovazione è correlato alla presenza di varie forze, sia interne che esterne. E gli studi legali sono solo alcuni fra i molti attori del settore.

Ciò dovutamente premesso, di seguito dieci elementi che, dal mio punto di vista, meritano riflessione, ed auspico possano stimolare riflessioni a livello di studi legali, policymakers, e altri stakeholder.

1. Struttura. L'architettura dominante degli studi legali italiani come associazioni di avvocati gioca un ruolo cruciale nella loro dinamica operativa. Questo rileva sia in termini di contabilità (contabilità per cassa vs. contabilità per competenza, il che influisce direttamente sugli investimenti tecnologici) sia di organizzazione interna (solitamente con molteplici comitati che devono approvare ogni specifico progetto – spesso con le loro deliberazioni e riserve –, tendenza a colli di bottiglia e propensione ad approcci gerarchici). Questo può causare ritardi, diluizione delle idee iniziali, o addirittura il completo rifiuto di idee a volte interessanti a causa della mancanza di consenso;

«La legge è anche, per natura, una professione conservatrice. Mentre una startup tecnologica tende a celebrare l'innovazione "disruptive", uno studio legale potrebbe vedere la "disruption" come una minaccia a processi collaudati nel tempo.»

2. Budget. Sebbene sia ovvio che l'innovazione richieda capitale, l'entità degli investimenti può variare enormemente. Un grande studio legale che intende creare un motore di ricerca basato sull'intelligenza artificiale o un piccolo studio legale che si abbona al suo primo software gestionale sono scenari molto diversi. Detto ciò, il budget è uno dei problemi più rilevanti, specialmente se guardiamo alla scala italiana ad ampio spettro. Sebbene un'analisi del budget negli studi legali nostrani richieda un intero libro per essere analizzata adeguatamente, vorrei sottolineare un fattore. Secondo l'ultimo rapporto sugli avvocati italiani, creato da Cassa Forense in collaborazione con il Censis[1], il reddito medio degli avvocati italiani è inferiore a 43.000 euro, e si attesta per le risorse più giovani (meno di 30 anni) a meno di 14.000 euro, e per quelle fascia mid (tra 31 e 40 anni) a meno di 26.000 euro.

1 *https://www.cassaforense.it/media/10560/rapporto-avvocatura-2023_blu_17-apr_def.pdf*

Considerando che una parte rilevante dello scenario degli studi legali italiani è costituita da sole practitioners, dovremmo riflettere su cosa significhi nella pratica un investimento tecnologico per la maggioranza degli avvocati italiani. Vorrei anche sottolineare che il fattore budget è fortemente influenzato dagli incentivi economici. Nonostante gli sforzi fatti da Cassa Forense, siamo molto lontani da un serio supporto agli avvocati e agli studi legali che intendono svoltare verso il digitale;

3. Mentalità degli avvocati. L'approccio degli avvocati tende ad essere – nella maggior parte dei casi – individualistico, non incline alla tecnologia e scettico con riguardo all'innovazione. Inoltre, la nostra tendenza al perfezionismo incide drasticamente sull'implementazione degli strumenti tecnologici. Quanti studi legali hanno reparti di ricerca e sviluppo? Quanti sono disposti ad avere 9 progetti che falliscono su 10? Quanti conoscono concetti come POC o beta test? La legge è anche, per natura, una professione conservatrice. Mentre una startup tecnologica tende a celebrare l'innovazione "disruptive", uno studio legale potrebbe vedere la "disruption" come una minaccia a processi collaudati nel tempo. Giusto a porre un esempio, pensiamo alle generazioni più esperte che si sono sempre affidate a libri e riviste cartacee. Come possono reagire a banche dati guidate dall'intelligenza artificiale? Non stupisce che il primo feedback siano preoccupazioni sull'affidabilità o autenticità;

4. Domanda da parte dei clienti. L'innovazione è spesso guidata dai nostri clienti. Se i clienti sono soddisfatti della tradizionale erogazione dei servizi, gli studi potrebbero non sentire l'urgenza di innovare. Quanti clienti chiedono agli studi legali di essere certificati ISO 27001? Di fare processi di due diligence con l'ausilio di legal tech? Di fornire assistenza generale combinando la consulenza fornita dagli avvocati e il supporto dei sistemi di intelligenza artificiale generativa? Se la clientela di uno studio è composta principalmente da clienti abituati a incontri faccia a faccia e revisioni fisiche di documenti, uno studio legale tende a non vedere la necessità di investire in migliori strumenti di collaborazione virtuale o sistemi di gestione documentale digitale;

5. Codice Deontologico degli avvocati. Gli standard etici a cui gli avvocati aderiscono sono radicati nella tradizione. Il nostro Codice Deontologico, nonostante sia relativamente recente, è considerato dalla maggior parte degli avvocati obsoleto.

Oltre ciò, è pensato prevalentemente attorno all'idea del sole practitioner che svolge attività di contenzioso, e tende a non considerare le sfide e gli obiettivi dei grandi studi legali. In questo momento, non abbiamo ancora regole riguardo l'adozione di sistemi di intelligenza artificiale, l'analisi predittiva dei giudizi e dei documenti, la copertura assicurativa in merito all'utilizzo erroneo di strumenti tecnologici. Gli avvocati non sanno se il loro dovere di competenza si estende all'adozione tecnologica, come la riservatezza è collegata al cloud, e molto altro;

«Il processo decisionale basato sui dati ha il potenziale per rivoluzionare il settore legale, consentendo agli studi legali di sfruttare l'analisi per la pianificazione strategica, l'identificazione di practice areas di interesse ed il miglioramento dei servizi offerti. Tuttavia, le complessità nel portare una cultura del dato all'interno degli studi legali, in particolare quelli italiani, sono molteplici, anche perché il concetto di cultura del dato va oltre i semplici numeri ed entra nelle nostre operazioni quotidiane.»

6. Narrative fuorvianti. Purtroppo, a volte i media presentano un'immagine distorta dell'innovazione negli studi legali italiani. Uno studio legale può fare un comunicato stampa riguardo l'adozione di un software tecnologico all'avanguardia, ma è frequente che questi tool siano utilizzati molto sporadicamente e solo per compiti specifici. Oppure potrebbero essere utilizzati solo da alcuni dipartimenti. Analogamente, i giornali possono parlare dell'analisi predittiva dei giudizi e del suo impatto sul sistema giustizia italiano come se fosse uno scenario già esistente su vasta scala. Questo crea aspettative irrealistiche per i clienti e pressioni per i professionisti;
7. Confronti errati. Stabilire paralleli con altri mercati, come Stati Uniti e Regno Unito, ma anche Singapore o Dubai, può essere controproducente. A causa delle risorse, della domanda dei clienti, della cultura tecnologica. Ma anche a causa del budget dei clienti e delle richieste di servizi legali. Inoltre, a causa delle differenze tra common law e civil law, i quadri normativi possono essere completamente diversi e i dipartimenti possono affrontare l'automazione in modo diverso;

8. Assenza di “evangelisti”. Senza player interni che spingono per l'innovazione, gli sforzi rischiano di essere vani. Inoltre, anche quando figure interne sono disposte a dedicare parte del loro tempo a progetti innovativi, non è scontato che abbiano il potere o le risorse per portarle avanti. Pensate a un giovane associate che scopre una piattaforma di legal tech perfetta per lo studio in cui lavora a una conferenza. Senza il coinvolgimento dei partner anziani come attori chiave per guidarne l'adozione, tale idea potrebbe rimanere in secondo piano;
9. Aspettative non realistiche. Una citazione erroneamente attribuita a Shakespeare recita che le aspettative sono la radice di tutti i mali. Nel 2017, con i primi software basati sull'intelligenza artificiale che arrivavano sul mercato legale italiano, si era diffuso un certo timore per robot che avrebbero sostituito il lavoro degli avvocati e dei giuristi d’impresa. Dopo diversi anni, lo scenario non è cambiato di molto. C'è molta paura, ma anche una sovrastima dell'effetto di un anno dell'intelligenza artificiale e della tecnologia sul campo legale italiano (sorprendentemente, c'è anche – almeno a mio parere – anche una sottostima degli effetti a 5 e 10 anni);
10. Carenza di cultura del dato. Il processo decisionale basato sui dati ha il potenziale per rivoluzionare il settore legale, consentendo agli studi legali di sfruttare l’analisi per la pianificazione strategica, l’identificazione di practice areas di interesse ed il miglioramento dei servizi offerti. Tuttavia, le complessità nel portare una cultura del dato all'interno degli studi legali, in particolare quelli italiani, sono molteplici, anche perché il concetto di cultura del dato va oltre i semplici numeri ed entra nelle nostre operazioni quotidiane. Non sorprende, pertanto, che si fatichi a trovare studi legali nei quali i dati non sono solo accessibili, ma anche valorizzati e utilizzati per guidare le decisioni.

Giuristi, studenti e fornitori possono interpretare lo scenario attuale sia con ottimismo che con scetticismo. Nonostante le sfide siano numerose, il lato positivo è l'innegabile progresso, in particolare dopo l'accettazione diffusa a seguito dell'ascesa dei modelli di intelligenza artificiale generativa.

Personalmente, rimango scettico riguardo alla metamorfosi degli studi legali in software house o di avvocati subitaneamente esperti in tecnologie all’avanguardia, principalmente

a causa degli ostacoli sopra indicati. Tuttavia, sono anche fiducioso che la familiarità con la tecnologia e l'innovazione miglioreranno nel breve e medio termine. Detto ciò, credo che l'obiettivo finale – in particolare per gli studi legali – non debba essere una trasformazione completa, ma una confidenza con la tecnologia e l'innovazione del 10 o 20% in più rispetto ai competitor. Coloro che raggiungeranno questo obiettivo sono pronti a dominare il mercato di domani.

L’OSINT NELL’ECOSISTEMA TECNOLOGICO MODERNO: ESPLORANDO LE PROFONDITÀ DELLE FONTI APERTE

Orazio Lacenere, Lacenere.it

INTRODUZIONE

Nel mondo digitale in rapida evoluzione, l’Open Source Intelligence (Osint) è diventato un pilastro essenziale per l’innovazione e la sicurezza in una varietà di settori e tecnologie avanzate. Dall'Intelligenza Artificiale ai Big Data, dalla Blockchain all’assicurazione cibernetica, l’Osint permea attraverso le complesse sfide del mondo moderno. In questo contesto, vogliamo esplorare le opportunità e le sfide offerte dall’Osint, usando esempi illuminanti che mettono in evidenza il suo ruolo fondamentale nell'era digitale.

L’OSINT NELL’INTELLIGENZA ARTIFICIALE

Nel campo dell’Intelligenza Artificiale, l’Osint diventa una risorsa chiave per addestrare modelli e comprendere il linguaggio umano. Ad esempio, analizzando conversazioni pubbliche online, l’Osint può migliorare la comprensione del linguaggio naturale degli algoritmi, aprendo la strada a applicazioni più sofisticate. Questo è solo un piccolo assaggio delle potenzialità dell’IA nelle fonti aperte.

L’OSINT E I BIG DATA

Nel mondo dei Big Data, l’Osint agisce come catalizzatore per l’arricchimento dei dataset. Raccogliendo dati aperti da una vasta gamma di fonti, organizzazioni e aziende ottengono una comprensione più dettagliata dei modelli di comportamento e delle preferenze degli utenti. Ciò fornisce una base solida per decisioni informate e strategie di business orientate al cliente.

L'OSINT NELLA BLOCKCHAIN

Nella Blockchain, l'Osint gioca un ruolo cruciale nella sicurezza delle transazioni. Analizzando le transazioni pubbliche, è possibile identificare schemi di comportamento sospetti, contribuendo a prevenire frodi e a mantenere l'integrità della rete. Questo è vitale per garantire la fiducia nelle transazioni digitali.

L'OSINT E LA SICUREZZA INFORMATICA

Nel campo della sicurezza informatica, l'Osint emerge come una risorsa cruciale per individuare potenziali minacce. Attraverso il monitoraggio di forum e siti web hacker, le organizzazioni possono anticipare gli attacchi informatici, adottando misure preventive per proteggere dati sensibili e infrastrutture critiche.

«Dall'Intelligenza Artificiale ai Big Data, dalla Blockchain all'assicurazione cibernetica, l'Osint permea attraverso le complesse sfide del mondo moderno.»

L'OSINT E LA PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE

Nella protezione della proprietà intellettuale, l'Osint permette la sorveglianza del mercato online per individuare prodotti contraffatti e violazioni dei diritti d'autore. Queste informazioni sono fondamentali per azioni legali tempestive, proteggendo gli interessi delle aziende e degli artisti.

L'OSINT E L'INTERNET DELLE COSE (IOT)

Nell'ambito dell'Internet delle Cose, l'Osint aiuta a identificare vulnerabilità nei dispositivi connessi. Analizzando pubblicamente le vulnerabilità note, esperti possono collaborare con i produttori per sviluppare soluzioni di sicurezza, proteggendo i consumatori da potenziali attacchi e intrusioni nella privacy.

L'OSINT NEL DESIGN LEGALE E NEL METAVERSO

Nel design legale, l'Osint analizza opinioni pubbliche e sentimenti online riguardo a questioni legali specifiche. Nel Metaverso, l'Osint monitora l'adozione di tecnologie

immersive, offrendo alle aziende una panoramica in tempo reale delle preferenze degli utenti. Questo guida lo sviluppo di esperienze metaversali coinvolgenti e innovative.

L'OSINT TRA DIGITALE E FATTORE UMANO

L'Osint rivela non solo dettagli comportamentali online, ma anche le dinamiche umane nel mondo digitale. Esplorando come idee e opinioni si diffondano attraverso piattaforme sociali, si catturano le sfumature delle relazioni umane, rivelando tendenze sociali ed emergenti. Questa comprensione è fondamentale per adattare tecnologie digitali alle necessità umane, creando soluzioni che rispecchiano la complessità della società moderna.

Attenzione però. Identificare la verità tra l'abbondanza di informazioni distorte e ingannevoli è diventato una missione critica, soprattutto per chi opera in questo campo.

Con l'avvento delle fake news e della manipolazione delle informazioni online, il tessuto stesso dell'Osint è minacciato. Fonti aperte e pubbliche, che un tempo rappresentavano una fonte affidabile di informazioni, possono ora essere compromesse, stravolte e manipolate per scopi nefasti. Questa distorta rappresentazione della realtà può influenzare negativamente le decisioni e le azioni basate su tali dati.

L'Osint, basandosi principalmente su queste fonti, è particolarmente vulnerabile a questa crescente minaccia. Riconoscere ciò che è autentico e ciò che è distorto richiede una preparazione e una conoscenza in profondità di questa disciplina. Gli esperti di Osint devono essere in grado di distinguere tra fonti affidabili e fonti manipolate, di valutare il contesto e di applicare metodi avanzati di verifica per filtrare la disinformazione dalla verità.

La preparazione in Osint non è solo una competenza auspicabile, ma una necessità assoluta. Gli analisti devono essere equipaggiati con un arsenale di tecniche sofisticate per sfidare la manipolazione delle informazioni. L'abilità di discernere tra fatti genuini e notizie false non solo preserva l'integrità dell'Osint, ma anche l'accuratezza e l'attendibilità delle informazioni riportate.

In un mondo in cui la verità può essere distorta con un click, l'Osint rappresenta un faro nella tempesta dell'informazione distorta. Ma questo faro deve brillare con una luce acuta e penetrante, alimentata dalla conoscenza approfondita e da prontezza

mentale e pensiero critico, come sostenuto dal dott. Giovanni Conio, esperto del settore intelligence, nell'articolo "Il pensiero critico nell'analisi intelligence" pubblicato sul sito del Dis (Dipartimento delle informazioni per la sicurezza).

Solo così si può sperare di navigare in modo sicuro tra le onde ingannevoli delle informazioni online, proteggendo così la verità e la fiducia nel mondo dell'intelligence aperta.

«La preparazione in Osint non è solo una competenza auspicabile, ma una necessità assoluta. Gli analisti devono essere equipaggiati con un arsenale di tecniche sofisticate per sfidare la manipolazione delle informazioni. L'abilità di discernere tra fatti genuini e notizie false non solo preserva l'integrità dell'Osint, ma anche l'accuratezza e l'attendibilità delle informazioni riportate.»

CONCLUSIONI

L'Osint si presenta come uno strumento potente nel mondo digitale contemporaneo, fornendo una visione unica sia delle dinamiche online che di quelle umane. Mentre offre nuove opportunità, pone anche sfide etiche e di privacy che richiedono una gestione attenta. Utilizzato in modo responsabile, l'Osint guida l'innovazione, migliora la sicurezza e contribuisce a plasmare un futuro tecnologico più sicuro, informato e centrato sull'umano per tutti noi. Questi appunti sono solo stimoli, invitandoci ad approfondire la comprensione di questo strumento potente nell'era digitale.

CYBERSECURITY: TENDENZE E IMPATTI SULLE AZIENDE NELL'ERA DIGITALE

Fabio Luinetti, Lodestar

Nell'era digitale, la cybersecurity è diventata una priorità strategica per tutte le aziende. Il continuo aumento delle minacce cibernetiche e l'evoluzione delle tecnologie stanno ridefinendo la gestione della sicurezza informatica. In questo articolo cercheremo di approfondire alcuni dei principali trend, le evoluzioni tecnologiche in ambito di cybersecurity e il loro impatto sulle aziende.

ATTACCHI INFORMATICI IN COSTANTE AUMENTO

Negli ultimi anni, l'aumento esponenziale degli attacchi informatici ha messo in evidenza la vulnerabilità delle aziende nell'era digitale. Gli attacchi ransomware, in particolare, rappresentano una delle minacce più insidiose. Questi attacchi, sempre più sofisticati, non solo criptano i dati aziendali, ma richiedono anche un riscatto per il loro ripristino, rendendo queste minacce ancora più pericolose. Gli hacker adottano tattiche più mirate, spesso prendendo di mira specifiche aziende o settori industriali. Questa evoluzione richiede una risposta altrettanto sofisticata, con una maggiore necessità di collaborazione intra-aziendale, attenzione alla protezione dei dati e alla preparazione per la gestione degli incidenti.

MINACCE ALLA DIGITAL FORENSICS

La disciplina delle Digital Forensics, che è fondamentale per raccogliere prove digitali utilizzate in procedimenti legali, è diventata un obiettivo per gli hacker. Gli aggressori

possono cercare di alterare o distruggere le prove digitali per minare l'integrità delle informazioni presentate in tribunale. Questo pone una pressione aggiuntiva sulla cybersecurity, che deve garantire la sicurezza delle prove digitali. Inoltre, la cybersecurity è strettamente legata alla validità delle prove digitali stesse, il che rende cruciale proteggerle adeguatamente.

TECNOLOGIE INNOVATIVE E IL LORO IMPATTO

Per rimanere competitive, molte aziende stanno adottando tecnologie innovative come ad esempio il cloud computing, l'Intelligenza Artificiale (IA) e l'edge computing. Queste tendenze hanno portato ad aumentare l'attenzione sulla sicurezza, poiché è fondamentale garantire la protezione dei dati e delle applicazioni ospitati nei cloud pubblici e privati.

«Gli attacchi informatici si sono evoluti per sfruttare le vulnerabilità nelle operazioni aziendali automatizzate e nelle supply chain, pertanto, la sicurezza informatica non è più un mero strato aggiuntivo, ma un componente fondamentale dell'automazione aziendale.»

L'IA e il Machine Learning (ML) stanno inoltre rivoluzionando anche la cybersecurity, consentendo di analizzare enormi quantità di dati per identificare comportamenti anomali e rilevare minacce in tempo reale. Inoltre, il modello Zero Trust Security sta guadagnando terreno, promuovendo l'idea che nessuna risorsa o utente, all'interno o all'esterno dell'azienda, debba essere implicitamente "fidato". Ogni richiesta di accesso deve essere verificata e autorizzata in base a criteri specifici, migliorando così la sicurezza complessiva dei sistemi.

AUTOMAZIONE E DIGITALIZZAZIONE DEI PROCESSI AZIENDALI

L'automazione dei processi aziendali è una tendenza chiave nell'era digitale. Le procedure di firma elettronica, l'archiviazione digitale e la gestione dei documenti contribuiscono a ridurre il carico di lavoro manuale, migliorando l'efficienza operativa. Tuttavia, questa

automazione espone le aziende a rischi informatici sempre più sofisticati. Gli attacchi informatici si sono evoluti per sfruttare le vulnerabilità nelle operazioni aziendali automatizzate e nelle supply chain, pertanto, la sicurezza informatica non è più un mero strato aggiuntivo, ma un componente fondamentale dell'automazione aziendale.

GESTIONE DEI RISCHI E CONFORMITÀ NORMATIVA

Le aziende sono costantemente esposte a rischi informatici, e la gestione di questi rischi richiede un approccio oculato. La creazione di team dedicati alla cybersecurity è diventata cruciale per sviluppare strategie di gestione dei rischi e risposte agli incidenti. Inoltre, la conformità normativa, come il GDPR in Europa, impone alle aziende di adottare misure di sicurezza informatica rigorose e di integrare la compliance normativa nei processi aziendali. Ciò comporta la necessità di collaborare strettamente tra team legali e tecnici per garantire la conformità alle normative e la protezione dei dati.

IMPATTO DEL COMPORTAMENTO DEI DIPENDENTI COME "CONSUMATORI" NEL MONDO DEL LAVORO

Un aspetto cruciale della cybersecurity aziendale è l'interazione tra il comportamento dei dipendenti come consumatori e le prassi aziendali. Spesso, le abitudini online dei dipendenti al di fuori dell'ambiente aziendale possono influenzare la sicurezza informatica sul posto di lavoro.

Gli stessi dipendenti che gestiscono con cura le proprie informazioni personali quando sono consumatori possono talvolta abbassare la guardia quando si tratta dei dati aziendali. Ad esempio, un dipendente che è cauto nell'evitare e-mail di phishing sul suo account personale potrebbe essere più incline a cliccare su un link sospetto su un account aziendale, soprattutto se non è stato adeguatamente formato sulla cybersecurity.

Inoltre, l'uso di dispositivi personali per attività aziendali, nota come "Bring Your Own Device" (BYOD), è diventato comune in molte aziende. Questo comporta un rischio aggiuntivo, poiché i dispositivi personali possono essere meno sicuri rispetto agli strumenti aziendali dedicati. Se i dipendenti non applicano le stesse misure di sicurezza sui loro dispositivi personali utilizzati per scopi aziendali, possono creare punti di

ingresso per gli attaccanti.

Le aziende devono quindi promuovere una cultura di sicurezza informatica che si estenda oltre i confini dell'ambiente di lavoro. I programmi di formazione e sensibilizzazione sulla cybersecurity dovrebbero affrontare non solo le pratiche aziendali, ma anche il comportamento dei dipendenti come consumatori. Questo approccio olistico contribuirà a ridurre i rischi e a creare una cultura di sicurezza in cui i dipendenti applicano le stesse buone pratiche sia a livello personale che professionale.

«Le aziende devono quindi promuovere una cultura di sicurezza informatica che si estenda oltre i confini dell'ambiente di lavoro. I programmi di formazione e sensibilizzazione sulla cybersecurity dovrebbero affrontare non solo le pratiche aziendali, ma anche il comportamento dei dipendenti come consumatori. Questo approccio olistico contribuirà a ridurre i rischi e a creare una cultura di sicurezza in cui i dipendenti applicano le stesse buone pratiche sia a livello personale che professionale.»

In ultima analisi, il comportamento dei dipendenti come consumatori ha un impatto diretto sulla cybersecurity aziendale. Gli individui che comprendono l'importanza della sicurezza informatica sia nella vita quotidiana che nel contesto aziendale contribuiranno a mitigare i rischi e a proteggere l’azienda dalle minacce cibernetiche in un mondo digitale sempre più complesso.

CAMBIAMENTO CULTURALE E COINVOLGIMENTO DEI DIPENDENTI

In virtù di quanto detto precedentemente, diventa evidente come la cybersecurity vada oltre le infrastrutture tecnologiche, richiedendo un cambiamento culturale all’interno delle aziende. Ogni dipendente deve essere coinvolto attivamente nella protezione dei dati aziendali. La consapevolezza e la formazione sulla sicurezza informatica sono essenziali.

Di fatto la cybersecurity è diventata un elemento fondamentale per la continuità aziendale e la sua reputazione, le aziende devono quindi promuovere una cultura

di sicurezza informatica in cui ogni individuo comprenda la sua responsabilità nella protezione dei dati aziendali. In un'epoca in cui le minacce cibernetiche evolvono rapidamente, l'adozione di un approccio proattivo e una stretta integrazione della sicurezza informatica nei processi aziendali sono essenziali. Le aziende che affrontano con successo queste sfide avranno un vantaggio competitivo, la resilienza alla cybersecurity è diventata un pilastro fondamentale per il successo aziendale nel mondo digitale di oggi.

CONCLUSIONI

In definitiva, tecnologie e comportamento degli utenti svolgono un ruolo fondamentale nella cybersecurity, sia nell'ambito aziendale che consumer.

L'educazione, la consapevolezza e l'adozione di buone pratiche di sicurezza sono essenziali per proteggere i dati, le informazioni legali e preservare l'integrità degli asset aziendali.

In un mondo sempre più digitale ed in continua evoluzione, la cybersecurity è una sfida condivisa che richiede un impegno costante da parte di aziende e individui.

La capacità di adattarsi ai cambiamenti tecnologici e comportamentali è fondamentale per garantire il successo delle aziende nell'era digitale.

L'INTELLIGENZA ARTIFICIALE AL BANCO DI PROVA DEL GDPR

Andrea Mantovani, Cleary Gottlieb Steen & Hamilton LLP

L'intelligenza artificiale è l'opportunità e la sfida del momento. Secondo stime di McKinsey del giugno 2023 ("The economic potential of generative AI: The next productivity frontier"), con 63 possibili utilizzi, l'intelligenza artificiale generativa potrebbe produrre tra 2,6 e 4,4 trilioni di dollari di benefici all'anno per l'economia.

Non vi sono solo i classici esempi delle smart city, dell'industria farmaceutica e della medicina predittiva, ma anche e sempre di più il settore legal tech: si pensi, tra tanti, all'uso dell'intelligenza artificiale per automatizzare la due diligence nelle operazioni di M&A.

Questo fenomeno impone attente riflessioni sulla data protection, perché l'intelligenza artificiale si alimenta spesso di dati personali: li raccoglie, li elabora e crea nuovi dati derivati, assumendo decisioni autonome che riguardano direttamente gli interessati cui i dati si riferiscono. Questo trattamento può essere massivo e opaco, rendendo difficile garantire il rispetto dei diritti individuali.

Non esiste ancora una normativa organica sull'intelligenza artificiale. La proposta di Regolamento europeo, noto come AI Act, è in fase di approvazione e il GDPR è il riferimento per gli aspetti connessi alla protezione dei dati personali.

Dopo i recenti interventi del Garante per la protezione dei dati personali – soprattutto nel caso ChatGPT – si è acceso un vivo dibattito sulla convivenza tra l'intelligenza artificiale e le regole di data protection del Legislatore europeo, come applicate dai Garanti nazionali.

Si afferma spesso che il rispetto della privacy – fra l'altro, in termini di minimizzazione del trattamento, trasparenza degli algoritmi e possibilità per gli interessati di esercitare i loro diritti – è oggi un'utopia per l'intelligenza artificiale, per la quale servirebbe una normativa ad hoc, più flessibile del GDPR.

A mio avviso, questa conclusione sarebbe eccessiva. Esistono utili indicazioni su come affrontare molti aspetti di questa complessa tematica di compliance. Fra l'altro, per citare una fonte, nella Guidance on AI and data protection dell'Information Commissioner's Office britannico.

«Dopo i recenti interventi del Garante per la protezione dei dati personali – soprattutto nel caso ChatGPT – si è acceso un vivo dibattito sulla convivenza tra l'intelligenza artificiale e le regole di data protection del Legislatore europeo, come applicate dai Garanti nazionali.»

È comunque vero che alcune aporie sembrano evidenti.

Per fare un esempio, un principio cardine del GDPR è l'esattezza dei dati personali (art. 5(1)(d)), che garantisce agli interessati il diritto di rettifica dei dati inesatti (art. 16). Tuttavia, l'intelligenza artificiale richiede per sua natura un periodo di rodaggio. L'esattezza si raggiunge con il tempo: all'inizio, i dati sono meno accurati; funzionando, il sistema li rende sempre più precisi.

Ipotizzando che una assoluta aderenza alle regole privacy non possa pretendersi – e non volendo però fermare il mondo in attesa di capire come fare – servirà una buona dose di inventiva nell'applicazione del GDPR al mondo dei sistemi di intelligenza artificiale.

Ad esempio, rispetto al tema dell'esattezza, se la rettifica immediata dei dati inaccurati inizialmente presenti nei sistemi di intelligenza artificiale fosse impossibile, l'esercizio del diritto degli interessati di ottenere la rettifica potrebbe ridursi a meccanismi che comportano tout court la cancellazione dei dati inesatti. Come è accaduto nel contesto degli impegni presi da OpenAI nel caso ChatGPT.

In quest'ottica di applicazione creativa del GDPR, diventa chiaramente centrale il duplice flusso di interlocuzione (i) fra autorità e titolari del trattamento che impiegano i sistemi

di intelligenza artificiale nonché (ii) fra le diverse autorità che applicano la normativa.

Sotto il primo profilo, l'interlocuzione è favorita dal principio di accountability (artt. 5(2) e 24 del GDPR). In base a tale principio, i titolari del trattamento che impiegano i sistemi di intelligenza artificiale devono prefigurare adeguate soluzioni di compliance, piuttosto che attendere puntuali prescrizioni dell'autorità. Come nel citato caso ChatGPT, ciò può tradursi in un dialogo volto a trovare un consenso dell'autorità su soluzioni – anche innovative sotto il profilo tecnologico o sotto quello relativo alla applicazione concreta delle norme – proposte dal titolare del trattamento.

«Anche la comunicazione fra i diversi Garanti della privacy europei è importante per assicurare un'interpretazione quanto più possibile uniforme, pur se innovativa.»

Anche la comunicazione fra i diversi Garanti della privacy europei è importante per assicurare un'interpretazione quanto più possibile uniforme, pur se innovativa. Sempre con riguardo a ChatGPT, nell'aprile 2023 i Garanti riuniti nel Comitato europeo per la protezione dei dati hanno lanciato una task force per promuovere la cooperazione e lo scambio di informazioni su iniziative per l'applicazione del GDPR.

Il coordinamento serve anche tra le diverse autorità nazionali. Infatti, queste tematiche non sono solo appannaggio del Garante per la protezione dei dati personali. Altre autorità, come l'Autorità garante della concorrenza e del mercato e l'Autorità per le garanzie nelle comunicazioni, applicano sempre più spesso la normativa sulla privacy quando incide su fattispecie di loro competenza.

Ad esempio, nell'aprile 2023, con riguardo a una tematica di grande interesse per i sistemi di intelligenza artificiale, il Garante privacy e l'Autorità per le garanzie nelle comunicazioni hanno istituito un tavolo congiunto, finalizzato alla promozione di un codice di condotta che conduca le piattaforme digitali ad adottare sistemi per la verifica dell'età degli utenti che accedono ai servizi online.

L'APPLICABILITÀ DELLA ZERO-KNOWLEDGE PROOF SULLA GESTIONE DELL'IDENTITÀ DIGITALE

Massimo Marabese, Cellularline Group

Una nuova tecnologia innovativa sulla gestione dell'identità digitale si sta facendo strada: la Zero-Knowledge Proof (ZKP). Con il termine "Zero Knowledge" si indica un tipo di crittografia sulle "dimostrazioni a conoscenza zero" con cui due parti possono mettersi d'accordo sulla veridicità di un'affermazione senza rivelare alcuna informazione sull'affermazione stessa. Gli algoritmi calcolano la probabilità che una parte, in una transazione, possieda un'informazione senza dover rivelare di cosa si tratta. I primi studi di Zero-Knowledge Proof a cui è possibile risalire sono cominciati negli anni '80 ad opera di alcuni ricercatori del MIT, Shafi Goldwasser, Charles Rackoff e Silvio Micali, tramite il concetto di "Knowledge Complexity of Interactive Proof Systems".

Esistono due tipi di algoritmi ZKP:

1. Interattivi: consistono in una serie di quesiti matematici che la parte ricevente deve risolvere;
2. Non interattivi: non comportano alcuna interazione tra le parti che effettuano la transazione o il processo di verifica, ma implica una funzione crittografica di hash come "controparte".

In ogni caso le dimostrazioni a conoscenza zero devono soddisfare tre condizioni:

1. Completezza delle informazioni: se un'affermazione è vera, la parte che verifica può confermare che la parte ricevente possiede un'informazione;
2. Solidità dell'informazione: una dichiarazione non può essere falsificata. Una parte

non può essere indotta con l'inganno a credere che l'altra possieda un'informazione se ciò non è vero;

3. Conoscenza zero delle informazioni: la parte verificante non è a conoscenza di altre informazioni oltre alla verità o falsità di una dichiarazione.

Aggiungere ZKP alla blockchain fornisce molti vantaggi. La blockchain di per sé fornisce già criteri di trasparenza, immutabilità e decentralizzazione. Tuttavia, essendo un sistema DLT (Distributed Ledger Technologies) ossia un registro distribuito che condivide le informazioni tra molteplici parti per verificare la validità delle transazioni, per definizione, può creare problemi inerenti la privacy e la sicurezza dei dati. La ZKP sopperisce proprio alla necessità di verificare l'autenticità delle transazioni senza rivelare i dati sottostanti. Quindi sempre di più gli sviluppatori hanno cominciato ad inserire algoritmi ZKP in soluzioni blockchain.

«Gli ultimi sviluppi in tema di digital identity hanno però l'obiettivo di riportare il pieno controllo dell'identità all'utente che la crea, grazie al modello della Self Sovereign Identity. Essere (ma soprattutto rimanere) "sovrani" esclusivi della nostra identità, significa poterla controllare e scegliere quali delle nostre informazioni personali condividere e con chi.»

Nel mondo attuale, i sistemi di verifica dell'identità sono oggi centralizzati ed il loro controllo è completamente affidato ad enti governativi o aziende terze alle quali è stato demandato questo cruciale compito. In ogni caso si tratta di sistemi che per quanto sicuri hanno inevitabilmente delle vulnerabilità, sono soggetti ad accessi non autorizzati o comunque ad abusi di utilizzo. Non solo: siamo tutti abituati a condividere le nostre informazioni personali per accedere a prodotti e servizi su Internet. Quotidianamente concediamo e distribuiamo i nostri dati e le nostre informazioni (anche in eccesso) a fornitori di servizi creando molteplici e numerose "identità digitali" su cui il nostro controllo è minimo. Non è infrequente il caso in cui per dimostrare ad esempio l'età o la residenza anagrafica ci venga richiesto di condividere integralmente un documento

di identità. In quel caso concediamo l'accesso a molte più informazioni rispetto a quelle necessarie (luogo e data di nascita, foto, numero del documento). Gli ultimi sviluppi in tema di digital identity hanno però l'obiettivo di riportare il pieno controllo dell'identità all'utente che la crea, grazie al modello della Self Sovereign Identity. Essere (ma soprattutto rimanere) "sovrani" esclusivi della nostra identità, significa poterla controllare e scegliere quali delle nostre informazioni personali condividere e con chi. La Self Sovereign Identity è un modello di identità digitale ideale. Alla base vi è il concetto, solo apparentemente banale, che l'identità debba sempre essere sotto l'esclusivo controllo dell'individuo che ne è rappresentato, il quale può disporne in modo indipendente, senza la necessità di affidarsi a intermediari terzi.

«La crittografia Zero Knowledge non solo viene utilizzata per garantire sicurezza e privacy, ma anche perché velocizza e rende più leggera l'elaborazione delle transazioni, spesso appesantita dalla mole di dati che devono essere registrati.»

La ZKP consente:

1. Totale indipendenza da organismi di autorità centrale che garantiscano l'identità personale, sostituita da prove crittografiche che ne certificano l'autenticità e la veridicità;
2. Eliminazione di frodi legate all'identità e di data breach;
3. Garanzia assoluta di privacy consentendo la condivisione di specifici attributi senza la necessità di rivelare ulteriori informazioni anche sensibili;
4. Scalabilità (inteso come fattore tecnico pratico) tramite un sistema computazionalmente efficiente per l'adozione su larga scala;

Ed infatti, ad esempio, nell'ambito delle criptovalute l'applicazione di questa crittografia è integrata nei meccanismi della blockchain. Si raggiunge l'accordo sulla validità delle transazioni senza esplicitare tutti i dati ogni volta. La crittografia Zero Knowledge non solo viene utilizzata per garantire sicurezza e privacy, ma anche perché velocizza e rende più leggera l'elaborazione delle transazioni, spesso appesantita dalla mole di

dati che devono essere registrati. In ambito DeFi (Decentralized Finance – i servizi di finanza decentralizzata che utilizzano le blockchain, a differenza dei servizi finanziari "centralizzati" forniti dalle banche e da altri istituti finanziari tradizionali, in cui agli utenti è permesso di utilizzare le criptovalute per usufruire di servizi comparabili a quelli erogati dalle banche tradizionali tramite le monete aventi corso legale emesse dai diversi paesi, come ad esempio concedere e ottenere prestiti, ottenere il pagamento di interessi, scambiare asset, acquistare polizze assicurative e molto altro) l'utilizzo della dimostrazione a conoscenza zero può essere fondamentale nel definire linee guida sovranazionali per i servizi finanziari su blockchain.

Alcuni altri esempi di applicazioni: i sistemi di messaggistica si basano sulla crittografia end-to-end per proteggere le comunicazioni. Ciò richiede agli utenti di verificare la propria identità utilizzando delle credenziali, mentre ZKP potrebbe verificare la validità delle credenziali senza effettivamente conoscerle. Nelle operazioni di voto ZKP può garantire che una persona sia idonea a votare senza rivelare la sua identità. Nei servizi pubblici invece, può essere usata in situazioni in cui gli utenti devono dimostrare l'idoneità senza rivelare informazioni sensibili. Altre forme di verifica potrebbero applicarsi anche alla gestione dell'identità, aggirando le complicazioni associate a passaporti, certificati di nascita, ed altri documenti. Mentre nel settore finanziario potrebbe essere utilizzato per verificare l'idoneità alla concessione di prestiti senza dover chiedere estratti conto o buste paga. Mentre negli smart contract si potrebbero sfruttare dati forniti da altre fonti per innescare determinate azioni senza richiedere l'accesso a informazioni sensibili.

In generale l'applicabilità di ZKP sta dimostrando di estrema versatilità e importanza nell'attuale panorama digitale.

LA PATERNITÀ DELL'OPERA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: TRA PROBLEMATICHE DI COPYRIGHT E DISINFORMAZIONE

Savino Menna e Fabio Azzolina, Studio LA&P

Chat-GPT, Bard, Gemini (e chi più ne ha, più ne metta!): nell'era della digitalizzazione e dell'intelligenza artificiale (IA) siamo sempre più esposti a contenuti generati da macchine, i quali possono assumere forme e contorni diversi. Negli ultimi anni, poi, complice anche il costante progresso tecnologico e la disponibilità di una sempre maggiore mole di dati, i modelli di IA sono diventati sempre più sofisticati e potenti, tanto da riuscire a generare contenuti il cui livello di precisione e complessità rasenta la perfezione di un'opera prodotta dall'essere umano (recenti studi ipotizzano che nel 2027 si raggiungerà la prima versione della c.d. "Single AI", dove la macchina arriverà addirittura a superarci).

La situazione appena descritta comporta spesso la difficoltà di distinguere l'opera dell'uomo da quella prodotta dalla macchina, con conseguenti problematiche connesse principalmente (seppur non in via esclusiva) al diritto d'autore e alla crescente diffusione delle fake news (con disinformazione galoppante annessa).

Ovviamente non tutti i mali vengono per nuocere ed il presente scritto non si propone di demonizzare tout court l'innovazione. Piuttosto vuole sensibilizzare la creazione di un pensiero critico per il lettore e creare consapevolezza nell'uso responsabile di certi strumenti, i quali, se ben compresi, possono realmente essere al servizio dell'uomo e non sostituirlo: pensiamo, infatti, che il progresso tecnologico abbia una base neutra, sta a noi arricchirla positivamente e non negativamente.

L'AUTENTICITÀ DELL'OPERA: PROBLEMATICHE ETICO-SOCIALI E SFIDE DELL'IA

Come accennavamo in premessa, la difficoltà di distinguere l'autenticità di un contenuto prodotto dall'IA piuttosto che dall'essere umano comporta problematiche di importante rilevanza, soprattutto se queste possono avere conseguenze ed impatti sociali.

Spesso, infatti, circolano e si diffondono in rete notizie false, create massivamente attraverso l'utilizzo delle macchine al fine di generare consensi, ingannare gli utenti e manipolare l'opinione pubblica.

La disinformazione è storia antica ormai (celebre la fake news sull'altezza di Napoleone), ma la sua evoluzione tecnologica è qualcosa di davvero allarmante: pensate che solo in Italia nel 2023 ci sono più di 100 siti internet che generano appositamente e quotidianamente notizie false, e ciò solo per attrarre "click" e arricchirsi attraverso i proventi pubblicitari connessi.

«Un'altra tematica attualmente "sotto i riflettori" della giurisprudenza nazionale ed internazionale riguarda la possibilità di riconoscere il diritto d'autore o di copyright in capo all'autore di opere prodotte attraverso sistemi di IA.»

Cosa importa se si aumenta la confusione all'interno di una società già attanagliata dalla costante infodemia? L'importante è guadagnare e sfruttare la massa popolare che spesso, complice l'assenza di pensiero critico, prende come oro colato quanto gli viene proposto dal web e social network.

Che dire poi delle rilevanti conseguenze che l'uso improprio dell'IA può produrre su copyright e diritto d'autore?

L'IA E L'INCERTEZZA DELLA PATERNITÀ DELLE OPERE NEL DIRITTO D'AUTORE

Data la continua evoluzione delle modalità di utilizzo dei sistemi di IA, ad oggi, risulta difficile individuare le tipologie di tutele giuridiche relative al diritto d'autore e al copyright che possono essere utilizzate nei confronti e/o a favore dei contenuti digitali creati dai sistemi di IA.

Per stabilire se le opere create attraverso i sistemi di IA possono determinare una violazione del diritto d'autore e di copyright altrui, occorre innanzitutto capire come tali opere vengono realizzate.

Infatti, i sistemi di IA creano contenuti attraverso algoritmi di Machine Learning, che consentono di sfruttare i dati di cui si alimentano (quali, immagini, testi, suoni) per "apprendere" dagli stessi e, sulla base di questi, creare nuove opere.

Il contenuto generato dall'IA sarà, quindi, frutto della combinazione dei dati di partenza utilizzati, con il rischio di presentare alcune somiglianze con gli stessi e, di conseguenza, di violare i diritti di proprietà intellettuale altrui.

«L'evoluzione tecnologica e lo studio scientifico, fortunatamente ad oggi hanno individuato alcune caratteristiche utili a distinguere, seppur non in maniera infallibile, l'opera prodotta dall'essere umano rispetto a quanto creato dall'IA.»

Pertanto, seppur ancora oggi oggetto di forte dibattito fra dottrina e giurisprudenza, per valutare la sussistenza o meno di una violazione dei diritti d'autore e di copyright, è opportuno verificare: (i) se gli autori dei dati utilizzati dai sistemi di IA abbiano fornito il loro consenso allo sfruttamento delle loro opere da parte delle società detentrici dei suindicati sistemi di IA; (ii) il livello di somiglianza tra il contenuto creato dall'IA e il "dato di partenza".

Un'altra tematica attualmente "sotto i riflettori" della giurisprudenza nazionale ed internazionale riguarda la possibilità di riconoscere il diritto d'autore o di copyright in capo all'autore di opere prodotte attraverso sistemi di IA.

Al riguardo, l'Ufficio del Copyright degli Stati Uniti si è recentemente pronunciato nel senso di non ritenere tutelabili dal diritto d'autore le opere d'arte realizzate attraverso le macchine.

Tuttavia, tale decisione non è stata totalmente condivisa da alcuni esponenti della dottrina statunitense, in quanto, secondo alcuni, prima di riconoscere o meno la paternità di un'opera creata attraverso sistemi di IA, dovrebbe essere valutata la complessità delle istruzioni impartite dall'artista al sistema di IA.

Analogamente, anche la nostra Corte di Cassazione, la quale ha recentemente disposto che l'elemento discriminante per stabilire se attribuire la paternità di un'opera prodotta attraverso l'IA a colui che si è avvalso di tale tecnologia consiste nella prevalenza dell'apporto umano alla realizzazione dell'opera stessa (ordinanza n. 1107/2023): "Dunque, nell'ipotesi in cui, all'esito di tale accertamento di fatto, venga ritenuto prevalente l'apporto umano rispetto a quello della macchina, non vi è ragione per non riconoscere tutela autorale alla persona che di tale strumento si sia servita".

Ciò descritto, pertanto, ben può comprendersi come ad oggi l'assenza di una normativa unitaria che disciplini la questione in maniera univoca e definitiva comporti ancora uno status di incertezza nel connubio IA e paternità delle opere prodotte.

QUALI SONO LE PRINCIPALI CARATTERISTICHE PER DISTINGUERE L'OPERA UMANA DA QUELLA ARTIFICIALE?

L'evoluzione tecnologica e lo studio scientifico, fortunatamente ad oggi hanno individuato alcune caratteristiche utili a distinguere, seppur non in maniera infallibile, l'opera prodotta dall'essere umano rispetto a quanto creato dall'IA.

Seppur molte delle stesse possono essere eluse dalle macchine più sofisticate, le principali metodologie si concentrano:

- Sul lessico: le opere dell'uomo tendono ad avere un linguaggio ampio e variegato, arricchito altresì da espressioni colloquiali, slang, doppi sensi, sfumature e termini specifici; quelle dell'IA, invece, tendono ad essere ripetitive e più limitate, utilizzando maggiormente parole comuni e generiche;
- Sulla sintassi: le opere dell'uomo tendono ad avere una struttura più complessa e imprevedibile, oltre ad incisi, subordinate e punteggiatura; quelle dell'IA, invece, tendono ad avere una struttura più semplice e rigida, con frasi più brevi e lineari;
- Sulla coerenza: le opere dell'uomo hanno solitamente una coerenza logica e tematica; quelle dell'IA, invece, tendono ad avere una coerenza superficiale e frammentaria, spesso con diverse contraddizioni;
- Sulla creatività: le opere dell'uomo sono creative ed originali, alle volte arricchite da metafore e un pizzico di humor; quelle dell'IA, invece, sono statiche e limitate, con idee banali, prevedibili e caratterizzate da serietà;

- Sugli errori: le opere dell'uomo possono contenere errori grammaticali o di battitura; quelle dell'IA, seppur pecchino di scarsa creatività, non presentano tale tipo di errori.

SOLUZIONI TECNOLOGICHE PRATICHE CHE VENGONO IN NOSTRO SOCCORSO

Veniamo poi alla parte più interessante del presente paper.

Esistono ad oggi soluzioni tecnologiche in grado di aiutarci a distinguere l'opera dell'uomo da quella della macchina?

Ovviamente sì, seppur, come accennato, non sono infallibili. Noi vi proponiamo il seguente elenco:

- Smodin è uno strumento online che offre un servizio di rilevamento dei contenuti IA multilingue. Le sue funzionalità si basano su algoritmi avanzati che confrontano il testo con diverse banche dati preesistenti, valutando unicità, lessico, sintassi e coerenza;
- AI Image Forensics è uno strumento creato da un organismo non profit europeo, che rileva le immagini generate da AI come StyleGAN, BigGAN e CycleGAN. Si basa su tecniche di analisi delle frequenze spaziali, che individuano le anomalie e le incongruenze tipiche delle immagini sintetiche;
- Fake News Detector è uno strumento sviluppato dall'Università di Pisa, che permette di identificare le notizie false generate da intelligenze artificiali come Grover, GPT-2 e GPT-3. Le sue funzionalità si basano su un modello di apprendimento che combina diverse caratteristiche (linguistiche, stilistiche e semantiche);
- Deepfake Detector è uno strumento realizzato dall'Università di Trento, che consente di riconoscere i video alterati da AI come DeepFaceLab, FaceSwap e Face2Face. Si basa su una rete neurale che analizza i volti dei soggetti e rileva le incongruenze tra le espressioni e movimenti facciali.

BREVI CONCLUSIONI

La sfida di distinguere tra l'opera prodotta dall'uomo e quella di derivazione artificiale non riguarda solo tecnologia e scienza, ma va ben oltre: rapporti sociali e diritti umani sono, infatti, al centro di questo radicale cambiamento generazionale.

Per tali ragioni è importante accrescere il nostro pensiero critico, verificare sempre le fonti delle informazioni che apprendiamo e promuovere una cultura della responsabilità e della trasparenza nell'uso delle intelligenze artificiali, sia da parte dei produttori che dei consumatori, garantendo l'autenticità dell'opera.

Solo così potremo sfruttare al meglio le potenzialità delle macchine senza perdere la nostra identità umana.

IL TRASFERIMENTO DEI DATI EXTRA U.E. È (STATO) ILLEGALE: BREVI CONSIDERAZIONI CRITICHE SUL NUOVO DATA PRIVACY FRAMEWORK

Nicola Nappi, Studio Legale Nappi

Durante il 2023 la Commissione Europea si è impegnata nuovamente a (tentare di) risolvere un intricato dilemma tramite un dettagliato documento di oltre 190 pagine: lo scambio di dati personali con gli Stati Uniti. Questo sforzo riflette la determinazione dell'Unione Europea nel tentare di trovare una soluzione a un problema considerato fino ad ora insolubile, e che vide, ormai diversi anni fa, chi scrive partecipare alla class action che portò alla prima storica decisione sul punto della Corte di Giustizia Europea[1].

È d'uopo un breve riepilogo.

Dieci anni orsono Edward Snowden rivelò che il governo degli Stati Uniti utilizzava le

1 *Il riferimento è alla class action che portò poi alla Sentenza della Corte di Giustizia dell'Unione Europea (Grande sezione), 6 ottobre 2015 Nella causa C-362/14, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, con la quale la Corte ha affermato che l'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.*

aziende Big Tech e programmi come "PRISM" o "Upstream" ai sensi della FISA 702 e della EO 12.333 per spiare il resto del mondo senza la necessità di una motivazione specifica o di un'approvazione giudiziaria. E tale attività non si limitava al contrasto alla criminalità o al terrorismo, ma includeva anche lo spionaggio sui "partner" degli Stati Uniti, come gli Stati membri dell'Unione Europea.

Peccato però che, già dal 1995, i dati personali dei cittadini europei non possono essere inviati al di fuori dell'U.E. a meno che non vi sia una protezione "sostanzialmente equivalente" nel paese di destinazione[2]. Sin da allora, infatti, l'immagine dell'Europa era quella di una fortezza assediata, intorno alla quale erigere barriere (immateriali) di difesa per preservare le attività economiche e produttive dalle intrusioni di aziende che operavano in paesi che non garantivano tutele equivalenti.

«Questa, che ben potremmo definire, e ci sia concesso, come una nuova versione del "Privacy Shield" (che a sua volta, come abbiamo visto, era una nuova versione del "Safe Harbor") è destinata in realtà ad avere una durata limitata, proprio come le due versioni precedenti. Infatti, il problema fondamentale non è stato affatto superato e dunque permane nei rapporti tra l'U.E. e gli Stati Uniti: la possibilità per le autorità governative americane di agire a proprio arbitrio sui dati dei cittadini degli Stati membri dell'Unione.»

Nel 2000 però, una decisione della Commissione Europea, passata alla storia con il nome di "Safe Harbor", dichiarò ufficialmente gli Stati Uniti in grado di fornire meccanismi di protezione "sostanzialmente equivalenti". Inutile dire che l'industria statunitense (e non

2 Il riferimento è alla Direttiva 95/46/CE, adottata il 24 ottobre 1995, con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali per garantire un "flusso libero" (free flow of data) dei dati e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini. La direttiva si occupava anche di regolamentare il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo (SEE), vietandolo nei casi in cui lo Stato di destinazione avesse un livello di protezione non adeguato alle norme europee. In pratica, tale direttiva ha cambiato radicalmente l'approccio precedente, che permetteva ogni trasferimento verso paesi terzi a meno che non emergessero problematiche. Da quel momento, invece, veniva adottata l'ottica opposta, stabilendo che nessun trasferimento fosse consentito a meno che il paese terzo non offrisse un adeguato livello di protezione.

solo) fece molto affidamento su tale decisione.

Ma nel 2015 per tali imprese arrivò la prima doccia fredda. A seguito della class action di cui dicevamo poche righe sopra, che portò alla causa C-362/14 ("Schrems I"), infatti, la Corte di Giustizia dell'Unione Europea annullò tale decisione della Commissione, muovendo le proprie considerazioni soprattutto della vastità di leggi di sorveglianza statunitensi che erano in evidente contrasto con i più elementari principi sulla privacy. Passò però pochissimo tempo e la Commissione europea approvò nuovamente la stessa e identica decisione sui trasferimenti di dati U.E.-U.S.A., ma con il nuovo nome di "Privacy Shield". Ma anche questa fu però successivamente invalidata nel 2020 dalla CGUE a seguito della causa C-311/18 ("Schrems II"), e in gran parte per gli stessi motivi della precedente.

E adesso, fatto questo doveroso riepilogo, e venendo ai giorni nostri, il 10 luglio 2023 la Commissione Europea ha emanato per la terza volta una decisione di adeguatezza, denominata stavolta "Data Privacy Framework". Inutile dire, anche in questo caso, come le aziende basate nell'Unione Europea, che hanno in un modo o nell'altro legami con le Big Tech, abbiano tirato un sospiro di sollievo alla notizia, ma, a sommesso avviso di chi scrive, tale sospiro è destinato a smorzarsi presto.

«L'applicazione del Data Privacy Framework sarà inevitabilmente laboriosa, burocratica e costosa, e non agevolerà in modo alcuno le attività delle aziende e delle istituzioni pubbliche.»

Questa, che ben potremmo definire, e ci sia concesso, come una nuova versione del "Privacy Shield" (che a sua volta, come abbiamo visto, era una nuova versione del "Safe Harbor") è destinata in realtà ad avere una durata limitata, proprio come le due versioni precedenti. Infatti, il problema fondamentale non è stato affatto superato e dunque permane nei rapporti tra l'U.E. e gli Stati Uniti: la possibilità per le autorità governative americane di agire a proprio arbitrio sui dati dei cittadini degli Stati membri dell'Unione.

È altamente probabile che, in un futuro prossimo, dopo le richiamate sentenze della Corte europea conosciute come "Schrems I" e "Schrems II", che hanno smontato le precedenti decisioni della Commissione, si arrivi ad una "Schrems III" che porterà

anche il nuovo testo alla stessa sorte dei due suoi predecessori. E questo causerà inevitabilmente e ancora una volta paura, incertezza e dubbi nell'ecosistema pubblico e privato che si affida alle Big Tech, oltre a finire inevitabilmente di rallentare il processo di transizione digitale. Le pubbliche amministrazioni e le aziende continueranno ad operare infatti sotto la minaccia di provvedimenti giudiziari o di Autorità nazionali di protezione, le quali ben potrebbero scoperchiare le fondamenta e scoprire, usando un'espressione Popperiana, i grattacieli di cristallo su palafitte di legno.

Senza volerci sostituire alle Autorità, e lungi da noi dal farlo, ci permettiamo evidenziare alcuni punti alquanto controversi emersi dalla lettura di queste 190 pagine. In particolare a pagina 35 è dato leggere: "U.S. intelligence agencies may seek access to such data for national security purposes (…) under the Foreign Intelligence Surveillance Act (FISA) (…) FISA contains several legal bases that may be used to collect (…) the personal data of Union data subjects transferred under the EU-U.S. DPF (Section 105 FISA222, Section 302 FISA223, Section 402 FISA224, Section 501 FISA225 and Section 702 FISA226)".

Ebbene, giova ricordare, e sembra incredibile doverlo fare, che fu proprio il FISA (e in particolare la Section 702, disposizione chiave del FISA Amendment Act del 2008 che consente al governo di condurre una sorveglianza mirata di persone straniere situate al di fuori degli Stati Uniti, con l'assistenza obbligata di fornitori di servizi di comunicazione elettronica, per acquisire informazioni di intelligence estera) ad essere una delle principali ragioni che portarono la Corte di Giustizia europea a invalidare il Privacy Shield. Ed oggi, come visto, tale richiamo ricompare pedissequamente anche nel Data Privacy Framework.

Non è tutto. Infatti, sempre nella stessa pagina, qualche rigo oltre, viene incredibilmente affermato che: "U.S. intelligence agencies also have possibilities to collect personal data outside the United States, which may include personal data in transit between the Union and the United States".

Ebbene, non possiamo esimerci dal sottolineare la portata di questo assunto. Cioè, non solo le autorità americane potranno accedere ai dati dei cittadini degli Stati membri dell'U.E. presenti nel loro territorio, ma potranno anche raccoglierli all'estero (dove loro non hanno giurisdizione e neanche l'U.E.). Ora, sia chiaro, non è certo una novità che gli U.S.A. abbiano spiato le istituzioni dei Paesi europei (e non solo), e il fatto che possano farlo solo con un ordine esecutivo del Presidente non cambia il fatto che gli Stati membri

dell'Unione non abbiano voce in capitolo.

Ed allora, a nostro sommesso avviso, ci sembrerebbe di poter giungere alla conclusione che la Commissione U.E. abbia semplicemente procrastinato il problema anziché risolverlo, generando così più complicazioni di quante ne abbia eliminate (o tentato di eliminare). L'applicazione del Data Privacy Framework sarà inevitabilmente laboriosa, burocratica e costosa, e non agevolerà in modo alcuno le attività delle aziende e delle istituzioni pubbliche. Inoltre, e forse questo è il punto più preoccupante, e richiamato nel titolo del presente contributo, tale decisione di adeguatezza va in un certo senso a sancire che fino al 9 luglio 2023 (e cioè al giorno prima della decisione della Commissione) non era consentito lo scambio di dati con gli Stati Uniti e che, logicamente, chiunque l'abbia fino ad allora fatto ha con ogni probabilità violato la legge.

«Ed allora, facendo buon governo dei principi sulla irretroattività delle leggi, le domande ci sorgono spontanee: perché le autorità nazionali di protezione dei dati non hanno mai bloccato tali trasferimenti? E soprattutto, ora che è stata approvata questa decisione, tali autorità avvieranno indagini volte a sanzionare coloro che fino ad oggi hanno utilizzato i servizi delle Big Tech (e di molti altri operatori statunitensi)?»

Ed allora, facendo buon governo dei principi sulla irretroattività delle leggi, le domande ci sorgono spontanee: perché le autorità nazionali di protezione dei dati non hanno mai bloccato tali trasferimenti? E soprattutto, ora che è stata approvata questa decisione, tali autorità avvieranno indagini volte a sanzionare coloro che fino ad oggi hanno utilizzato i servizi delle Big Tech (e di molti altri operatori statunitensi)?

Ma in fin dei conti, qualunque saranno le scelte delle Autorità, esse saranno piene di conseguenze negative: se dovessero infatti decidere di indagare, allora saranno costretti a irrogare sanzioni a destra e a manca a causa dell'inerzia politica sia a livello comunitario che nazionale; ma se dovessero scegliere di non indagare, a nostro avviso, potrebbero arrecare un danno irreparabile alla fiducia nel primato della legge, poiché certificheranno che, in nome delle necessità politiche, il diritto deve arretrare.

La Commissione Europea ha mostrato, ancora una volta, scarsa attenzione per lo stato di diritto e la privacy dei suoi cittadini. Questo terzo tentativo di far passare in gran parte la stessa decisione illegale solleva anche interrogativi sul ruolo più ampio della Commissione Europea come custode dei trattati dell'U.E. Invece di sostenere lo "Stato di diritto", la Commissione si limita ad approvare più volte una decisione non valida, nonostante le chiare sentenze della Corte di Giustizia dell'Unione Europea. Nonostante la grande indignazione suscitata dalle rivelazioni di Snowden nell'U.E. e i ripetuti inviti del Parlamento Europeo (l'ultimo a maggio di quest'anno[3]) e del Garante Europeo per la protezione dei dati (l'ultimo a febbraio di quest'anno) ad agire, la Commissione sembra dare la priorità alle relazioni diplomatiche con gli Stati Uniti e alle pressioni commerciali su entrambe le sponde dell'Atlantico rispetto ai diritti dei cittadini europei e ai requisiti del diritto dell'Unione Europea.

Mai come nel caso della nuova decisione di adeguatezza, quindi, la soluzione proposta è peggiore del problema stesso.

3 *European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)*

LEGAL REVOLUTION: DALLA TRASFORMAZIONE DIGITALE ALL'INTELLIGENZA ARTIFICIALE

Rosalba Oliva, EUforLEGAL

Negli ultimi decenni, il settore legale ha subito una trasformazione epocale grazie all'innovazione tecnologica. La digitalizzazione e l'adozione di strumenti basati sull'intelligenza artificiale (AI) stanno rivoluzionando il modo in cui le direzioni legali d'azienda gestiscono le loro operazioni quotidiane, migliorando l'efficienza, la precisione e la tempestività nella fornitura dei servizi legali a tutto tondo. L'informatizzazione e la digitalizzazione hanno cambiato negli anni diversi settori e anche quello legale non può esimersi da questo cambiamento: le competenze digitali "di base" sono già lo strumento indispensabile per ogni professione, anche quella dell'avvocato!

TRASFORMAZIONE DIGITALE NEL SETTORE LEGALE

La trasformazione digitale nel settore legale è stata un processo graduale ma inevitabile. Gli uffici legali, una volta caratterizzati da procedure cartacee e manuali, stanno abbracciando la digitalizzazione per migliorare la loro efficienza e adattarsi alle nuove esigenze.

Non si tratta di superare il tradizionale ruolo dell'avvocato, ma di fare un salto di qualità nel proprio lavoro verso una più efficiente attività grazie alle opportunità della digitalizzazione. Un avvocato che evolve nel ruolo verso l'avvocato digitale.

Queste sono solo alcune delle attività che beneficiano delle opportunità offerte dalla tecnologia:

1. Gestione documentale digitale: una delle prime aree a beneficiare della digitalizzazione è stata la gestione dei documenti. Le soluzioni di gestione documentale consentono di archiviare, organizzare e condividere documenti in modo più efficiente, riducendo al minimo il rischio di smarrimento o errore umano;

2. Comunicazione e collaborazione online: le piattaforme di comunicazione e collaborazione online hanno rivoluzionato il modo in cui gli avvocati interagiscono con tutti gli stakeholders (interni ed esterni all'organizzazione). Questi strumenti permettono di condividere informazioni in tempo reale e di lavorare in modo sincronizzato, indipendentemente dalla posizione fisica;

3. Automatizzazione dei processi giuridici: l'automatizzazione dei processi giuridici, attraverso l'uso di software specializzati, consente di ridurre il carico di lavoro manuale. Ad esempio, i documenti standard possono essere generati automaticamente, i promemoria possono essere programmati e i processi di ricerca legale possono essere accelerati grazie all'accesso a database online.

«Non si tratta di superare il tradizionale ruolo dell'avvocato, ma di fare un salto di qualità nel proprio lavoro verso una più efficiente attività grazie alle opportunità della digitalizzazione. Un avvocato che evolve nel ruolo verso l'avvocato digitale.»

INTELLIGENZA ARTIFICIALE E MACHINE LEARNING NEL SETTORE LEGALE

L'adozione dell'Intelligenza Artificiale e del Machine Learning sta portando ulteriori miglioramenti nelle strutture legali. Queste tecnologie consentono di affrontare sfide complesse e migliorare la qualità dell'attività lavorativa e delle performance legali.

1. Analisi predittiva: l'AI può analizzare grandi quantità di dati legali storici (tabellari, testuali, immagini scansionate, ecc.) per individuare tendenze, modelli e pattern nascosti. Questo può essere utile nella previsione dei tempi e costi di lavorazione delle pratiche, nella valutazione dei rischi fino ad un'analisi statistica avanzata di

previsione degli esiti;

2. Ricerca avanzata & discovery: gli strumenti di ricerca legale basati sull'AI e sul Linguaggio Naturale (NLP) consentono agli avvocati di accedere rapidamente a precedenti giurisprudenziali, leggi e giurisprudenze pertinenti, accelerando il processo di ricerca e analisi;
3. Automatizzazione del contratto: l'AI può automatizzare il drafting e la revisione dei contratti, individuando clausole importanti, termini e condizioni che richiedono attenzione. Ciò riduce i tempi di redazione del contratto, accelera la negoziazione contrattuale, la compliance normativa e minimizza il rischio di errori;
4. Assistenza legale virtuale: le interfacce conversazionali e gli assistenti virtuali basati sull'AI e sui sistemi di Large Language Model (simili a ChatGPT) possono fornire risposte immediate a domande legali (Question & Answering). Questi strumenti migliorano l'accessibilità all'informazione legale.

«I vantaggi della modernizzazione dei processi – dai più operativi fino alle decisioni strategiche – sono sempre più concreti ed è facile immaginare che sempre più professionisti e strutture legali cercheranno l'aiuto della tecnologia per migliorare la produttività, avere maggiori elementi decisionali e allo stesso tempo elevare il lavoro del professionista legale.»

SFIDE E PUNTI APERTI

Nonostante i numerosi vantaggi, l'adozione dell'AI nel settore legale non è priva di sfide. Il principale punto aperto riguarda la sicurezza dei dati, poiché le informazioni legali sono estremamente sensibili e devono essere protette rigorosamente ed in conformità alle normative vigenti. L'introduzione dell'AI nel trattamento delle pratiche legali deve inoltre essere conforme alle direttive Europee in materia di Etica, Responsabilità, Spiegabilità e Rischi degli algoritmi (Artificial Intelligence Act). Anche nei processi completamente digitalizzati e automatizzati riveste particolare importanza la presenza di punti di controllo da parte degli specialisti (Human in the loop). Le decisioni finali devono essere sempre prese dagli avvocati.

CONCLUSIONI

La trasformazione digitale e l'integrazione dell'intelligenza artificiale stanno ridefinendo il settore legale, migliorando l'efficienza operativa, il processo decisionale e la qualità dei servizi offerti.

I vantaggi dela modernizzazione dei processi – dai più operativi fino alle decisioni strategiche – sono sempre più concreti ed è facile immaginare che sempre più professionisti e strutture legali cercheranno l'aiuto della tecnologia per migliorare la produttività, avere maggiori elementi decisionali e allo stesso tempo elevare il lavoro del professionista legale. È essenziale trovare un equilibrio tra l'automazione e l'esperienza umana per garantire una pratica legale di successo ed eticamente responsabile.

EUforLegal Srl (Gruppo Eustema) da anni opera nel settore del Legal Tech. I risultati degli investimenti in Ricerca & Sviluppo della Scienza 4.0, applicata alla digitalizzazione e automazione dei processi, hanno traguardato la realizzazione degli spunti forniti nel presente testo implementati in soluzioni di mercato quali: Teleforum For, Minerva for Legal e Certo, già adottati da diversi enti pubblici e organizzazioni private.

Le nostre soluzioni e applicazioni di legal AI abbracciano tre direttrici funzionali ed estraggono conoscenza preziosa da una quantità elevata di dati eterogenei, svolgendo un ruolo fondamentale per l'avvocato, con l'obiettivo di:

1. Automatizzare le attività svolte in maniera manuale per aumentare il rendimento e la produttività, agevolando le attività durante la conduzione delle pratiche legali (LegalAutomation);
2. Supportare le scelte strategiche per una più efficiente gestione dei processi, grazie ad avanzate funzionalità di ricerca di concetti, entità, parole semanticamente simili, citazioni, riferimenti legislativi, anche su documenti e contenuti non strutturati (LegalDiscovery);
3. Creare valore aggiunto ai processi aziendali esterni alla struttura legale, contribuendo a individuare punti di miglioramento, azioni correttive e rischi/benefici annessi per visualizzare in modo semplice e intuitivo una mole smisurata di dati eterogenei tramite dashboard avanzate (LegalAnalytic).

IP E METAVERSO: GLI UFFICI MARCHI INTRODUCONO NUOVE CLASSI PER I PRODOTTI VIRTUALI E GLI NFT, MENTRE L'EUIPO SI OCCUPA DEI MARCHI NEL METAVERSO

Laura Orlando, Herbert Smith Freehills

La dodicesima edizione della Classificazione di Nizza, entrata in vigore il 1° gennaio 2023, ha introdotto nuove categorie per la registrazione dei marchi per tutelare gli NFT ed è oggi utilizzata da diversi uffici marchi nazionali nonché dall'EUIPO. Anche l'Ufficio per la Proprietà Intellettuale del Regno Unito (UKIPO) ha redatto delle nuove linee guida.

In particolare, nella nuova edizione della Classificazione di Nizza è stata inclusa una nuova voce nella Classe 9: "file digitali scaricabili autenticati da token non fungibili". Questa voce è stata inserita proprio a causa del numero sempre maggiore di domande di registrazione di marchi inerenti a termini relativi a prodotti virtuali e token non fungibili (NFT) presentate in tutto il mondo.

Il Metaverso rappresenta senza dubbio una nuova era per i depositi di marchi a tutela di "prodotti virtuali". La continua espansione di questa nuova realtà virtuale ha sollevato questioni fondamentali relative alla tutela dei diritti della proprietà intellettuale e dei marchi e ha spinto fashion major come Louis Vuitton, Nike e Crocs a depositare nuove domande di marchio per tutelare tutti i servizi relativi al proprio business nel Metaverso.

Tradizionalmente, un marchio che contraddistingue scarpe è protetto nelle classi 25 e 18 (quest'ultima è rivendicata in quanto i prodotti inclusi sono considerati simili a quelli appartenenti alla classe 25). Recentemente, si è assistito ad un aumento delle domande di marchio per proteggere prodotti virtuali scaricabili e NFT. Ciò in quanto non era per nulla chiaro se le classi 25 o 18 fossero appropriate per scarpe di carattere

esclusivamente virtuale (ossia progettate per essere indossate da "avatar" digitali nel Metaverso e non nel mondo reale).

Si pensi a tal proposito al recente tentativo di Burberry di registrare il proprio pattern a scacchi rosso e nero per contraddistinguere beni e servizi nel Metaverso. Il caso è interessante in quanto l'EUIPO nella pronuncia emessa in data 8 febbraio 2023 si è espresso in merito al requisito del carattere distintivo di un marchio per prodotti virtuali, ritenendo che, ai fini della valutazione della distintività, sia possibile applicare le regole e i principi applicabili ai marchi tridimensionali.

«Il Metaverso rappresenta senza dubbio una nuova era per i depositi di marchi a tutela di "prodotti virtuali". La continua espansione di questa nuova realtà virtuale ha sollevato questioni fondamentali relative alla tutela dei diritti della proprietà intellettuale e dei marchi e ha spinto fashion major come Louis Vuitton, Nike e Crocs a depositare nuove domande di marchio per tutelare tutti i servizi relativi al proprio business nel Metaverso.»

UNIONE EUROPEA

Il 31 marzo scorso, l'EUIPO ha pubblicato delle linee guida per chiarire come classificare i prodotti sopra citati e quale debba essere l'approccio adottato dall'ufficio in linea con i principi consolidati di classificazione dei beni e dei servizi.

L'EUIPO ha espressamente chiarito che la classe 9 è quella appropriata per i "prodotti virtuali", poiché essi sono trattati come contenuti digitali o immagini. Tuttavia, in applicazione della sentenza IP Translator della Corte di Giustizia dell'UE (CGUE), il termine "prodotti virtuali" di per sé può mancare di chiarezza e precisione e, pertanto, deve essere ulteriormente specificato indicando il contenuto a cui si riferiscono i prodotti virtuali (ad esempio, "prodotti virtuali scaricabili, ossia abbigliamento/calzature digitali"). Al momento della registrazione di un marchio per gli NFT, i richiedenti devono specificare il tipo di articolo digitale autenticato tramite NFT, ad esempio "musica scaricabile autenticata da NFT".

Nel frattempo, vi è stato un tentativo di proteggere il termine "METAVERSE" come

marchio nell'UE. La seconda Commissione Ricorsi dell'EUIPO ha affrontato per la prima volta la questione in due recenti decisioni riguardanti i marchi METAVERSE FOOD (R2357/2022-2), nelle classi 5, 29, 30 e 32 e METAVERSE DRINK (R2356/2022-2), nella classe 32. L'EUIPO ha respinto entrambe le domande per mancanza di carattere distintivo. Il richiedente ha impugnato la decisione sostenendo che le domande non si riferivano a prodotti virtuali ma a beni fisici nel mondo reale. La Commissione Ricorsi ha respinto i ricorsi ritenendo che il termine "METAVERSE" si riferisse a uno spazio virtuale. I segni avevano il significato di "cibo in uno spazio virtuale" e "bevande in uno spazio virtuale". Inoltre, secondo la Commissione Ricorsi, il termine "METAVERSE" non si riferirebbe solo ad avatar, realtà alternative e prodotti virtuali, ma rappresenterebbe anche un'altra versione di commercio elettronico. Su questa base, la Commissione Ricorsi ha ritenuto che i marchi sarebbero intesi come indicazioni che i prodotti sono offerti o possono essere acquistati in uno spazio virtuale e che "METAVERSE FOOD" e "METAVERSE DRINK" non saranno percepiti come un'indicazione di origine commerciale, ma solo come informazioni di carattere generale sui prodotti in questione.

«Considerando il fatto che, come detto inizialmente, la dodicesima edizione della Classificazione di Nizza attribuisce una posizione specifica degli NFT all'interno della classe 9, ciò potrebbe implicare che tutti i marchi che non includono questa classe tra quelle rivendicate non possano essere fatti valere contro l'uso di NFT.»

Queste decisioni della Commissione Ricorsi permettono di concludere che il termine "METAVERSE" è da intendersi come termine descrittivo e non distintivo e quindi non può essere monopolizzato e registrato da un unico soggetto. Alla luce di ciò e tenendo conto delle decisioni citate, cosa accadrà ai vari marchi costituiti o contenenti la parola "METAVERSE" che sono stati in precedenza concessi dall'EUIPO? Applicando il ragionamento della Commissione Ricorsi a questi marchi e a marchi simili, essi dovrebbero essere considerati non distintivi e quindi soggetti ad azioni di nullità. Al momento, attendiamo di vedere come l'EUIPO ha intenzione di risolvere queste incongruenze.

REGNO UNITO

Anche nel Regno Unito, l'UKIPO il 3 aprile 2023 ha emanato delle linee guida specifiche sulla classificazione delle domande di marchio per gli NFT, i prodotti virtuali e i servizi forniti nel Metaverso, con lo specifico intento di aiutare coloro che desiderano registrare un marchio per prodotti o servizi nel Metaverso. In linea con quanto previsto dalla dodicesima Classificazione di Nizza, ad esempio, l'ufficio inglese potrebbe rifiutare le domande di registrazione marchio aventi ad oggetto il termine NFT in quanto del tutto generico e vago e potrebbe richiedere, inoltre, ai titolari di specificare nel dettaglio l'attività a cui si riferisce il termine NFT. In linea con la decisione del Tribunale italiano nel caso Juventus, che ha riconosciuto la contraffazione di un marchio anche in relazione al minting di un NFT (vedi infra), le corti del Regno Unito potrebbero ritenere che il minting e la commercializzazione di NFT che riproducono un marchio registrato nel Metaverso possano ancora violare tale marchio registrato sulla base di un vantaggio sleale ai sensi dell'articolo 10(3) dell'UK Trade Marks Act 1994 (UKTMA). Un motivo alternativo di protezione per i marchi "ben noti" può essere l'articolo 56 dell'UKTMA, che fornisce una protezione aggiuntiva per tali marchi.

ITALIA

In Italia, come sopra anticipato, il Tribunale di Roma nel caso Juventus[1] ha emesso una importante decisione che rappresenta secondo alcuni una pietra miliare della protezione della proprietà intellettuale in relazione agli NFT, ai beni virtuali e al Metaverso in Europa. Nel caso trattato, alla luce di un'interpretazione estensiva dei principi esistenti, il Tribunale di Roma ha stabilito, per la prima volta, che il minting di un NFT (come qualsiasi altra attività commerciale) incorporante un marchio richiede il consenso preventivo e l'autorizzazione del titolare del marchio. Considerando il fatto che, come detto inizialmente, la dodicesima edizione della Classificazione di Nizza attribuisce una posizione specifica degli NFT all'interno della classe 9, ciò potrebbe implicare che tutti i marchi che non includono questa classe tra quelle rivendicate non possano essere fatti valere contro l'uso di NFT. In contrasto con tale sviluppo dell'EUIPO, la decisione del Tribunale di Roma potrebbe quindi fornire un po' di conforto ai titolari dei marchi, ammettendo un'applicazione estensiva delle classi rivendicate.

1 *https://hsfnotes.com/ip/2023/01/10/nft-infringes-trade-mark-rights-finds-italian-court-in-juventus-case/*

COME CHATGPT, GENAI E LLM INFLUENZERANNO IL FUTURO DELLA LEGGE PER AVVOCATI E NON AVVOCATI

Hans Paul Pizzinini, Speedlegal[1]

Il diritto, professione intrinsecamente legata al linguaggio, è fiorito per secoli sulla precisione del suo gergo per garantire chiarezza e coerenza. Guardando al futuro, i progressi nei Large Language Models (LLM), nella Generative Artificial Intelligence (GenAI) e nel più ampio dominio dell'Artificial Intelligence (AI) prefigurano profonde trasformazioni nel panorama legale, in particolare per i non avvocati.

CAPIRE LLM, GENAI E AGI

Gli LLM, rappresentati da modelli come GPT, LLaMa e Alpaca, sono radicati nel mondo dell'AI. Più specificamente, sono un sottoinsieme dei modelli di Deep Learning conosciuti come modelli Transformer. Questi modelli, distinti per i loro vasti parametri, sono abili nel prevedere e generare sequenze di parole. Per questo, sono definiti large.

Potete pensare ai modelli pre-LLM come a un bibliotecario che ci indirizza alla giusta sezione della biblioteca, allo scaffale giusto, e ci può raccomandare alcuni titoli. Un LLM, invece, è come un bibliotecario esperto che può ricordare dettagli di ogni pagina di ogni libro della biblioteca e può dare spiegazioni a qualsiasi nostra domanda, basate su tutto ciò che ha letto e compreso.

1 *https://speedlegal.io/*

Storicamente, l'analisi del testo si basava principalmente sulle Reti Neurali Ricorrenti (RNN). Queste reti, pur essendo efficaci nell'analizzare sequenze di testo, presentavano alcune limitazioni portando spesso a tempi di elaborazione prolungati. Tuttavia, con l'introduzione dell'architettura dei Transformer 2017, il panorama del Natural Language Processing (NLP) ha subito una svolta radicale. I modelli di Machine Learning (ML) basati sui Transformer hanno non solo migliorato la precisione dell'analisi del testo, ma hanno anche accelerato notevolmente i tempi di elaborazione, rivoluzionando così l'approccio al trattamento delle informazioni linguistiche.

GenAI, un'applicazione degli LLM, è dedicata alla generazione di nuovi dati attraverso la replicazione di set di dati esistenti. Nel dominio legale, questo si traduce ad esempio in attività come la stesura di contratti, la creazione di domande di brevetto e l'offerta di consigli legali tramite chatbot o altri strumenti. GenAI non deve essere confuso con l'intelligenza artificiale generale (AGI) – una forma di AI in grado di replicare qualsiasi attività intellettuale umana.

«Potete pensare ai modelli pre-LLM come a un bibliotecario che ci indirizza alla giusta sezione della biblioteca, allo scaffale giusto, e ci può raccomandare alcuni titoli. Un LLM, invece, è come un bibliotecario esperto che può ricordare dettagli di ogni pagina di ogni libro della biblioteca e può dare spiegazioni a qualsiasi nostra domanda, basate su tutto ciò che ha letto e compreso.»

L'EVOLUZIONE DEL LEGAL TECH: POTENZIARE I NON AVVOCATI

Il linguaggio giuridico è fondamentale per contratti e procedimenti legali. Il suo vocabolario intricato serve come base di chiarezza e protezione nelle trattative legali. Tuttavia, LLM e GenAI stanno sfidando questo status quo. Questi avanzamenti non stanno solo ridefinendo come usiamo e comprendiamo il linguaggio giuridico; stanno democratizzando l'accesso alle informazioni e agli strumenti legali.

Tecnologie come la classificazione del testo e la Named Entity Recognition (NER) hanno già fatto breccia nella tecnologia legale, facilitando l'elaborazione e la categorizzazione automatica di enormi quantità di testi legali. Il Legal Tech, un campo in rapida espansione, abbraccia una moltitudine di strumenti:

- Piattaforme di gestione del ciclo di vita del contratto: gestiscono l'intero ciclo di vita di un contratto, dalla sua creazione alla sua scadenza o terminazione;
- Piattaforme di revisione e analisi dei contratti: consentono una rapida analisi dei contratti, evidenziando potenziali problemi, suggerendo correzioni e aree di negoziazione;
- Software Ediscovery: strumenti che aiutano a trovare, raccogliere e produrre informazioni memorizzate elettronicamente (ESI) come prova in cause legali;
- Software di gestione della pratica: soluzioni complete per la gestione delle informazioni sui clienti, dei casi, della fatturazione e altro ancora.

Sebbene molti di questi strumenti fossero inizialmente creati esclusivamente per il dominio dei professionisti legali, l'emergere degli LLM e della GenAI sta rendendo il diritto più accessibile e user-friendly per il grande pubblico. La linea tra strumenti legali professionali e quelli per la persona comune sta diventando sempre più sfumata, segnando un nuovo capitolo nel dominio dell'assistenza legale.

«Questi avanzamenti non stanno solo ridefinendo come usiamo e comprendiamo il linguaggio giuridico; stanno democratizzando l'accesso alle informazioni e agli strumenti legali.»

SFIDE FUTURE PER I TEAM LEGALI

- Gestione dei dati e conformità: con l'aumento dei dati generati e archiviati dalle aziende, gestire, ordinare, analizzare questi dati, garantirne la sicurezza e renderli disponibili per l'e-discovery in caso di contenzioso è diventato una sfida;
- Privacy dei dati, regolamentazione e conformità: con la rapida crescita della tecnologia, salvaguardare le informazioni sensibili e rimanere conformi alle normative sulla privacy in evoluzione è fondamentale. C'è stato un aumento delle normative sulla privacy (come il GDPR in Europa e il CCPA in California), sulla cybersecurity e su altre questioni legate alla tecnologia. I team legali devono rimanere aggiornati su queste normative, comprenderne le implicazioni e garantire che i loro clienti

rimangano conformi.

- Evoluzione tecnologica e integrazione della tecnologia: l'emergere dell'AI, della blockchain e di altre tecnologie offre opportunità e sfide. I team legali devono comprendere le implicazioni di queste tecnologie, specialmente in aree come la proprietà intellettuale, il diritto dei contratti e le questioni di responsabilità. Inoltre, l'integrazione organica di queste nuove tecnologie nei flussi di lavoro legali tradizionali può essere impegnativa.
- Preoccupazioni etiche con l'AI e la tecnologia: mentre i team legali iniziano ad adottare l'AI per compiti come la revisione dei contratti o la previsione degli esiti dei contenziosi, ci sono preoccupazioni etiche sulla trasparenza, l'equità e la responsabilità di questi sistemi AI.

INTEGRAZIONE DI LLM NEL SETTORE LEGALE: PUNTI DI RIFLESSIONE

L'integrazione degli LLM nel dominio legale è una prospettiva promettente, ma è complessa:

- Allucinazione: una grande preoccupazione riguardo agli LLM è l'"allucinazione", dove il modello potrebbe generare informazioni false o fuorvianti. In un contesto legale, ciò può avere gravi conseguenze, dalla errata interpretazione delle leggi a consigli giuridici scorretti;
- Limitazioni dei dati: con l'aumento della sofisticatezza dei modelli AI, acquisire testi legali di qualità per addestrarli diventa una sfida. I documenti legali sono spesso sensibili, confidenziali e non facilmente accessibili, rendendo difficile reperirli in grandi quantità;
- Imperativo dei dati di qualità: utilizzare fonti di dati legali accurate, aggiornate e imparziali è essenziale. Fare affidamento su testi legali obsoleti o errati potrebbe propagare principi legali obsoleti o incorretti.

Alla luce di queste sfide, molti esperti propongono misure per migliorare l'affidabilità degli LLM. Una di queste soluzioni è il metodo "Rewrite and Rollback" (R&R). Questo metodo permette continue revisioni dei dati, assicurando che i modelli rimangano

accurati. Utilizzando R&R, non solo si può mantenere l'accuratezza del modello, ma si può migliorare la qualità generale dei testi prodotti, beneficiando sia gli scrittori umani che la creazione di dati.

«La combinazione di strumenti avanzati, capacità di calcolo più accessibile, un maggior volume di dati, modelli open source e una crescente competenza nel campo dell'AI stimolerà innumerevoli innovazioni.»

COME SARANNO I PROSSIMI 12 - 48 MESI?

Nei prossimi 12 mesi assisteremo ad un crescente interesse verso applicazioni basate sui foundational models (LLM), come ad esempio strumenti AI per la stesura e revisione di contratti.

48 mesi da ora potrebbe divenire comune assistere ad agenti AI che negoziano contratti al nostro posto, relegandoci al ruolo di semplici osservatori. Suona come fantascienza? Lo sembra, ma potrebbe diventare realtà prima di quanto si pensi. Immagina di poter comunicare al tuo agente legale AI le condizioni che desideri e quelle su cui non sei disposto a transigere. Questo agente, basandosi sui tuoi input, elaborerà una strategia di negoziazione, confrontandosi con un agente AI della controparte dotato delle stesse capacità. L'accordo finale emergerebbe da un equilibrio determinato dai criteri stabiliti da entrambi.

Credo che, nei prossimi 12 mesi, l'intermediazione dell'uomo avrà ancora un ruolo preponderante rispetto all'automazione dei modelli AI. Tuttavia, nel lungo termine (oltre 48 mesi), il contributo umano diventerà progressivamente meno centrale man mano che la tecnologia sarà in grado di gestire compiti sempre più complessi. Queste tecnologie evolute saranno capaci di elaborare una vasta gamma di dati simultaneamente, tra cui aspetti dalle diverse sfaccettature come il carattere di un individuo e le preferenze personali.

Mi aspetto che le aziende del futuro ridefiniscano il proprio settore attraverso l'impiego dell'intelligenza artificiale. Un esempio contemporaneo di questo è TikTok, che ha rivoluzionato l'esperienza dei contenuti grazie a un'AI personalizzata. La combinazione di strumenti avanzati, capacità di calcolo più accessibile, un maggior volume di dati, modelli

open source e una crescente competenza nel campo dell'AI stimolerà innumerevoli innovazioni. Se la prima generazione di software (Software 1.0) si basava su codice creato manualmente e la seconda (Software 2.0) si focalizzava sul labelling dei dataset, il Software 3.0[1] vedrà al centro la modifica e l'ottimizzazione dei foundational models come gli LLM.

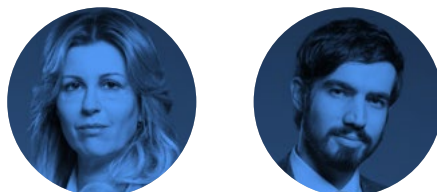
La professione legale è destinata a una profonda evoluzione, in cui l'expertise giuridica si fonderà con competenze tecnologiche avanzate. Gli strumenti Legal Tech e gli LLMs potrebbero presto diventare "consulenti legali di primo contatto", capaci di analizzare vaste quantità di informazioni e fornire consigli preliminari. Successivamente, saranno gli avvocati a perfezionare e concludere la consulenza. Nel frattempo, le implicazioni etiche della tecnologia prenderanno il sopravvento nelle discussioni, focalizzandosi sul ruolo dell'AI nella presa di decisioni e sulla sua capacità di garantire esiti equi e corretti.

CONCLUSIONE

In conclusione, l'integrazione di LLMs e GenAI nel campo legale porta con sé la promessa di una maggiore efficienza e precisione. Sebbene gli LLMs rappresentino una prospettiva entusiasmante per il settore legale, non dobbiamo dimenticare l'importanza del discernimento umano. La sfida sarà trovare il giusto equilibrio tra le capacità tecnologiche e il giudizio critico umano.

1 *https://sarahguo.com/blog/conviction*

BLOCKCHAIN E INDICAZIONI GEOGRAFICHE: LA TUTELA DEI SEGNI DI QUALITÀ AGROALIMENTARE NELL'ERA DEL WEB3

Monica Riva e Andrea Bardi, Legance - Avvocati Associati

LE RELAZIONI TRA BLOCKCHAIN E INDICAZIONI GEOGRAFICHE: "CONTROLLI INTERNI" E "TRACEABILITY"

Le indicazioni geografiche (IG) individuano il legame tra un nome e un territorio, che conferisce al prodotto finale caratteristiche organolettiche o, più semplicemente, una reputazione.

Secondo il considerando n. 46 del reg. (UE) n. 1151/2012 (il "Regolamento"), "il valore aggiunto delle indicazioni geografiche [...] si basa sulla fiducia dei consumatori. Esso è credibile solo se accompagnato da verifiche e controlli effettivi". E proprio a proposito dei controlli, la blockchain può rivelarsi utile a garantire il rispetto degli standard produttivi delle IG (c.d. "controlli interni"), i quali sono contenuti in un documento denominato "disciplinare di produzione" (il "Disciplinare"). A tal riguardo, l'art. 54 del Regolamento prevede che si possa procedere alla cancellazione della denominazione protetta dal registro ad opera della Commissione qualora "non sia più garantito il rispetto delle condizioni stabilite dal Disciplinare".

In questo ambito, la blockchain può trovare margini di applicazione rilevanti, potendo essere impiegata per gestire in modo efficiente e automatizzato le informazioni da fornire all'autorità accreditata per i controlli: ogni spostamento di un prodotto tra le varie fasi della filiera produttiva può essere annotato nel registro pubblico distribuito della blockchain.

Pensiamo al caso del formaggio DOP "Parmigiano Reggiano". Ai sensi del Disciplinare, il prodotto che si fregerà della DOP dovrà rispettare, inter alia, i seguenti requisiti: a) il latte deve essere consegnato al caseificio "entro due ore dalla fine di ciascuna mungitura";

b) il latte può essere raffreddato "immediatamente dopo la mungitura e conservato ad una temperatura non inferiore a 18° C"; c) la zona di produzione comprende "i territori delle province di Bologna alla sinistra del fiume Reno, Mantova alla destra del fiume Po, Modena, Parma e Reggio nell'Emilia".

Sembra dunque possibile, per i produttori della DOP Parmigiano Reggiano, inserire tutte le informazioni relative a vari passaggi della filiera all'interno del ledger (i.e. il registro)[1] della blockchain, assicurando una tracciabilità inalterabile e sicura dei dati, concernenti appunto la provenienza del prodotto, la temperatura di conservazione, il rispetto delle scadenze stabilite nel disciplinare. Ciò può favorire la conoscenza precisa e accurata di ogni fase della produzione, offrendo assoluta garanzia di trasparenza alle autorità di controllo e ai consorzi.

«E proprio a proposito dei controlli, la blockchain può rivelarsi utile a garantire il rispetto degli standard produttivi delle IG (c.d. "controlli interni"), i quali sono contenuti in un documento denominato "disciplinare di produzione".»

Questo utilizzo della tecnologia blockchain potrebbe essere ulteriormente integrato dall'applicazione degli smart contracts.

Lo smart contract è un "programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse".[2]

Quando lo smart contract riceve l'input pre-programmato (come ad esempio un avvenuto pagamento o il verificarsi di una condizione), esegue automaticamente e inesorabilmente l'ulteriore contro-prestazione.

Tornando all'esempio del Parmigiano Reggiano, potrebbero essere inseriti nella blockchain

1 *Il registro è, solitamente, liberamente consultabile da chiunque. Anche le persone fisiche, infatti, se dotate di una rete internet, possono accedere ad un blockchain explorer (e.g. etherscan.io), ove risultano reperibili, tramite apposite queries, tutte le informazioni pubbliche relative a transazioni, indirizzi wallet, smart contracts etc.*

2 *Art. 8-ter della l. n. 12/2019.*

– attraverso lo scanning di tags RFID[3] e/o l'impiego di sensori[4] – tutti i passaggi relativi alla lavorazione del prodotto (compresa la temperatura di conservazione o la provenienza della materia prima), collegando questi input ad uno smart contract, di modo che la catena produttiva possa essere automaticamente interrotta qualora uno dei requisiti previsti nel Disciplinare non fosse rispettato.

LE RELAZIONI TRA BLOCKCHAIN E INDICAZIONI GEOGRAFICHE: "CONTROLLI ESTERNI" ED "ENFORCEMENT"

La blockchain può essere utilizzata anche per i "controlli esterni". Ad esempio, può essere impiegata presso i supermercati, o presso ogni fornitore e rivenditore finale, per far sì che i prodotti non vengano accettati al momento della consegna se non risultano conformi al Disciplinare. La vendita dei prodotti agroalimentari protetti da DOP o IGP potrebbe dunque avvenire solo nel caso in cui siano rispettati i seguenti due requisiti: a) la conferma della ricezione fisica delle merci e b) un output dello smart contract che convalidi la conformità dei prodotti al Disciplinare o ai manuali d'uso.[5]

«In questo settore, dunque, la tecnologia blockchain sembra poter avere uno sviluppo significativo, tanto è vero che esistono già numerosi esempi di utilizzo in via sperimentale ai fini della lotta alla contraffazione.»

Qualora il prodotto agroalimentare non avesse un numero di lotto compatibile con i prodotti validati, i fornitori, ovvero i consumatori in possesso di lettore di qr-code o simili, potrebbero immediatamente rendersi conto della violazione, verificando se i passaggi

---

3 L'identificazione a radiofrequenza (RFID) è una tecnologia che consente di identificare in modo univoco gli oggetti tramite onde radio. A differenza di altri sistemi come i codici a barre o i codici QR, che utilizzano le immagini per l'identificazione, la RFID utilizza appunto le onde radio per catturare le informazioni dalle etichette RFID, per cui è solo essenziale che l'etichetta RFID si trovi nel raggio di lettura del lettore o dell'antenna RFID.

4 I sensori, debitamente connessi ad una rete Internet, potrebbero rilevare automaticamente la temperatura, la composizione chimica, la provenienza e altri dati chiave del prodotto che sarebbero poi inseriti su un registro di una blockchain. Cfr. A. Versetti, EUIPO Blockchain Observatory Forum, EUIPO Blockchain Conference, 19 febbraio 2019, pp. 41-42.

5 Cfr. S. Aronzon, Blockchain and Geographical Indications: A Natural Fit?, in papers.ssrn.com, p. 26.

della filiera siano o meno stati effettuati correttamente.

In questo settore, dunque, la tecnologia blockchain sembra poter avere uno sviluppo significativo, tanto è vero che esistono già numerosi esempi di utilizzo in via sperimentale ai fini della lotta alla contraffazione. In particolare, nel settore vitivinicolo ha destato una certa attenzione la partnership tra la blockchain Cardano e il rinomato produttore Georgiano Baia's Winery, finalizzata a classificare le fasi produttive del vino e a imprimere sulle bottiglie un qr-code (apposto dalla società Scantrust) che i consumatori possono scansionare al fine di verificare l'autenticità del prodotto[6]. I dati saranno naturalmente custoditi on-chain, garantendone l'immutabilità.

6 Cfr. https://blog.scantrust.com/case-study-baias-wine-anti-counterfeiting-and-supply-chain-awareness-on-the-cardano-blockchain/

IL LEGAL DESIGN COME STRATEGIA DI PREVENZIONE DEL CONTENZIOSO MEDICO-LEGALE

Maria Livia Rizzo, Studio Legale Stefanelli&Stefanelli

L'EVOLUZIONE DEL CONTENZIOSO MEDICO-LEGALE

In Italia, a partire dall'entrata in vigore del Codice civile del 1942, le azioni giudiziarie nei confronti dei medici si sono mantenute sporadiche per alcuni decenni, per poi aumentare in maniera tale da condizionare progressivamente l'operato dei clinici e delle stesse strutture, spesso influendo sulle scelte di politica sanitaria nazionale.[1]

I dati più recenti[2], presentati da Consulcesi al Ministero della Salute, rivelano 300.000 cause pendenti contro i camici bianchi con una media di 35.000 azioni legali intentate ogni anno in Italia.

Negli ultimi trent'anni l'aumento esponenziale della litigation ha consolidato nella classe medica un atteggiamento difensivo provocato non solo dalla preoccupazione per eventuali cause legali, ma anche dal timore di compromettere la propria carriera o la propria immagine, o di subire un procedimento disciplinare. Ciò vale tanto più per i professionisti influenzati da precedenti esperienze di contenzioso a carico proprio o di colleghi.

Le conseguenze dannose di questa condotta cautelativa sono note[3]: elevatissimi costi a

---

1 *Bruno G. e Tucci G. La gestione dell'errore – vero o presunto – in medicina. La tutela assicurativa nella responsabilità professionale medica, in Tagete, 2-2005; anno XI 1-14.*

2 *https://www.consulcesi.it/news/i-numeri-del-contenzioso-legale-medici-pazienti/*

3 *U.S. Congress, Office of Technology Assessment. Defensive medicine and clinical practice, OTA – H – 602, Washington DC, US Government Printing Office, 1994*

carico del Servizio Sanitario Nazionale dovuti alla sovrabbondanza di trattamenti e ricoveri inutili e di procedure diagnostiche invasive non necessarie, che peraltro causano stress emotivo nei pazienti ("medicina difensiva positiva").

Oppure si verifica il fenomeno opposto, ma ugualmente deleterio: il rifiuto di curare determinati pazienti – escludendoli dai trattamenti, soprattutto in ambito chirurgico, oltre le normali regole di prudenza – per evitare di eseguire procedure ritenute ad alto rischio ("medicina difensiva negativa").

Eppure, gli esiti delle azioni giudiziarie sembrano raccontare un'altra realtà: nel 95% dei casi i professionisti sanitari vengono prosciolti nei procedimenti penali, e nel 66% dei contenziosi civili la loro responsabilità non viene riconosciuta.

«Negli ultimi trent'anni l'aumento esponenziale della litigation ha consolidato nella classe medica un atteggiamento difensivo provocato non solo dalla preoccupazione per eventuali cause legali, ma anche dal timore di compromettere la propria carriera o la propria immagine, o di subire un procedimento disciplinare.»

In assoluto, la scienza medica non è una scienza esatta: gli errori vengono commessi, possono essere lamentati, riscontrati e valutati, e devono essere, conformemente a ciò, risarciti.

Ma i numeri citati svelano uno scenario molto più complesso.

Dietro alle cifre del contenzioso (e soprattutto ai relativi proscioglimenti) è possibile intravvedere una problematica che va al di là della diligenza e della perizia del professionista, e che oltrepassa anche l'esito fausto o infausto dell'intervento o della terapia.

IL RUOLO CARDINE DELLA COMUNICAZIONE MEDICO-PAZIENTE

La chiave di lettura di questo fenomeno risiede nel rapporto sempre più conflittuale tra medicina e società. Una conflittualità che sarebbe banale ed erroneo associare al concetto semplicistico di "malpractice".

Infatti, il livello medio di qualità dell'assistenza sanitaria in Italia è stato ripetutamente riconosciuto tra i più elevati al mondo[4] [5].

Al contrario, a incrementare la litigiosità è la mancata instaurazione di un rapporto di fiducia tra professionista sanitario e persona assistita. La causa deve essere ricercata, in particolare, nella relazione di gratitudine-risentimento intercorrente tra medico e paziente. Si tratta di una relazione da sempre conflittuale ma che in passato era contraddistinta da una conflittualità più attenuata[6]. Negli ultimi decenni, invece, il contenzioso è incardinato in una "animosità che rasenta l'irrazionale"[7] anche quando manca un vero e proprio danno.

A contribuire a questa diffidenza è in primis una difficoltà nella comunicazione medico-paziente sul trattamento proposto, sulle eventuali alternative terapeutiche e sulla possibilità di rifiuto.

Il colloquio clinico risente della originaria asimmetria informativa tra i due soggetti, e ha come esito una carenza o inadeguatezza di indicazioni fornite al malato.

Infatti, i pazienti che ritengono di aver subito un danno si rivolgono agli avvocati perché non sono riusciti ad ottenere una spiegazione dal proprio medico.

Del resto, la letteratura di settore[8] ha dimostrato che in media i professionisti sanitari sottostimano l'ammontare di informazioni che i pazienti vorrebbero ricevere. In alternativa, pur concordando con l'approccio descritto, lamentano la scarsità del tempo a loro disposizione e riconoscono in molti casi una carenza delle proprie attitudini comunicative.

Proprio per questo, se da un punto di vista teorico le abilità del medico necessarie a coinvolgere il paziente sono ben definite, molto meno agevolmente si riscontrano nella pratica clinica quotidiana.

Peraltro, l'incorporazione della centralità della persona nel Servizio Sanitario Nazionale

4 https://www.thelancet.com/journals/lanpub/article/PIIS2468-2667(19)30189-6/fulltext

5 https://www.agenas.gov.it/bandi-di-concorso/bandi-di-concorso-espletati?view=article&id=511:bloomberg&catid=115#:~:text=Terzo%20posto%20per%20il%20sistema,per%20Singapore%20e%20Hong%20Kong

6 *Mafrici O. Responsabilità professionale e contenzioso medico-legale, inTagete 2-2004; anno X: 1-13*

7 *Vinci P. Il medico è solo; Tagete 2-2006; anno XII: 1-10*

8 *Guadagnoli E. e Ward P. Patient participation in decision making, in Soc Sci Med, 1998; 47: 329-339*

italiano affronta oggi anche le sfide legate alla trasformazione dell'assistenza sanitaria dopo il Covid-19 nel complesso panorama della governance decentralizzata[9].

Ma già negli anni Novanta del secolo scorso le pubblicazioni scientifiche valorizzavano la comunicazione nel contesto clinico, sul presupposto che essa migliorasse gli outcome del paziente, diminuendone, di conseguenza, le rimostranze[10].

Proprio per questo motivo negli USA – dove è si è manifestato per la prima volta l'aumento della litigation per poi diffondersi in Europa, fino a raggiungere livelli preoccupanti – è stato elaborato il concetto di "patient-centered communication".

«A contribuire a questa diffidenza è in primis una difficoltà nella comunicazione medico-paziente sul trattamento proposto, sulle eventuali alternative terapeutiche e sulla possibilità di rifiuto.
Il colloquio clinico risente della originaria asimmetria informativa tra i due soggetti, e ha come esito una carenza o inadeguatezza di indicazioni fornite al malato.»

L'attenzione non è più limitata alla malattia e ai suoi aspetti fisiologici, ma investe anche il contesto psicologico e sociale in cui il paziente si trova[11], il suo punto di vista, lo scambio delle idee e la condivisione dei poteri e delle responsabilità[12].

La tradizione anglosassone insegna, in particolare, che quando esistono più opzioni di trattamento, per coinvolgere il paziente in un processo decisionale condiviso (shared decision-making) il professionista sanitario deve possedere determinate abilità. Tra

9 Cardinali F. et al. A nationwide participatory programme to measure person-centred hospital care in Italy: results and implications for continuous improvement. Health Expectations, 2021; 00:1–13

10 Stewart M et al. Patient-centered medicine: transforming the clinical method, in Thousand Oaks, Calif: Sage Publications; 1995

11 Epstein R. Patient-centered communication and diagnostic testing, in Annals of Family Medicine, 2005; Vol. 3, No. 5

12 Epstein R. et al. Measuring patient-centred communication in patient-physician consultations: theoretical and practical issues, in Soc Sci Med, 2005; 61:1516-1518

queste emerge la capacità di esporre all'assistito le evidenze cliniche, sollecitandolo ad esprimere le proprie preferenze e valutandone la compatibilità con le opzioni di trattamento disponibili[13].

Ma questo traguardo non può essere raggiunto se il paziente non è reso pienamente consapevole.

Il medico ha il compito di comunicare al paziente nel modo più chiaro possibile – accertandosi che le abbia comprese – le informazioni tecniche sulle opzioni di cura e i probabili rischi e benefici, aiutandolo a soppesarli senza imporgli i propri valori[14].

«Sul piano giuridico informare il malato è necessario per garantire il rispetto del suo diritto alla autodeterminazione. Tuttavia, i moduli di consenso il più delle volte sono gestiti come una mera "liberatoria preoperatoria" per l'esenzione da responsabilità, e sono talmente complessi da non facilitare affatto l'esercizio di questo diritto.»

RIVOLUZIONARE L'APPROCCIO AI DOCUMENTI GIURIDICI IN SANITÀ: IL LEGAL DESIGN

Il tipico terreno di prova per la sfida della patient-centered communication è il momento in cui l'assistito riceve, per sottoscriverli, i documenti propedeutici all'esecuzione della prestazione sanitaria.

Si tratta delle spiegazioni cliniche che accompagnano il modulo per l'acquisizione del consenso informato al trattamento medico e l'informativa sul trattamento dei dati personali.

Sul piano giuridico informare il malato è necessario per garantire il rispetto del suo diritto alla autodeterminazione. Tuttavia, i moduli di consenso il più delle volte sono gestiti come

13 *Elwyn G., et al. Shared decision making and motivational interviewing: achieving patient-centred care in Ann Fam Med, 2014, 12 (3): 270-275*

14 *Politi M. et al. Implementing clinical practice guidelines about health promotion and disease prevention through shared decision making. J Gen Int Med, 2013, 28(6):838-44*

una mera "liberatoria preoperatoria"[15] per l'esenzione da responsabilità, e sono talmente complessi da non facilitare affatto l'esercizio di questo diritto.

Tanto è vero che, come evidenziava Barni[16] già nel 2006, "il giudice ha da tempo mangiato la foglia e non si accontenta davvero di un autografo frettolosamente richiesto e stilato".

Il cardine della questione è che un'informazione carente priva il paziente del controllo sulla propria situazione clinica e gli impedisce di elaborare una scelta consapevole: e la responsabilità di garantire una informed choice incombe su chi fornisce la prestazione di cura.

Ciò vale anche per la privacy policy,[17] laddove una eccessiva complessità del testo non si traduce solo in una difficoltà di comprensione da parte dell'utente, ma anche in un rischio di non conformità per chi ha somministrato le informazioni.

Infatti, sul piano della protezione dei dati, il Considerando 58 del Reg. UE 679/2016 (GDPR) prevede che "le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione".

Inoltre, quando l'interessato non viene messo in grado di capire come il titolare del trattamento utilizza i suoi dati, non è neppure in grado esercitare, riguardo agli stessi, i diritti che il GDPR gli riconosce agli artt. 15-22.

Ma è impossibile fornire un'informazione adeguata senza porsi dal punto di vista del paziente, dovendosi intendere con "paziente" la persona assistita "non addetta ai lavori", priva di cognizioni tecnico-scientifiche o giuridiche e in alcuni casi penalizzata da barriere linguistiche e limiti culturali.

È, in definitiva, impossibile fornire un'informazione adeguata senza mettere il paziente al

15 Brenner L. e Brenner A. Beyond informed consent. Educating the patient, in Clin Orthop Relat Res, 2009, 467:348-351

16 Barni M. Posizione di garanzia del medico, dissenso (scritto) del paziente: crisi di due capisaldi della medicina difensiva, in Riv. It. Med. Leg., 2006; 2: 399 ss

17 Per un approfondimento sul legal design applicato alle informative privacy si veda Haapio et al. Legal Design Patterns for Privacy in Erich Schweighofer et al. (Eds.), Data Protection / LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018. Editions Weblaw, Bern 2018, pp. 445–450 (ISBN 978-3-906940-21-2) and in Jusletter IT, 22 February 2018

centro.

Per farlo, dalle spiegazioni cliniche o legali devono essere eliminati concetti articolati e termini tecnici, per fronteggiare non solo l'eventuale incomprensione della lingua o un basso grado di scolarizzazione, ma anche semplicemente una conoscenza non specialistica della materia.

La vera sfida è superare la complessità delle parole senza sacrificarne il significato e gli obiettivi.

La strategia consiste nell'abbandonare il wall of text per adottare l'approccio visuale introdotto dal legal design.

«Non si tratta di una semplice trasformazione del testo in immagine: bisogna assicurare che il significato originario e l'interpretazione finale coincidano.»

La metodologia del legal design consiste in una applicazione dello human-centered design al settore legale e ha come scopo quello di riprogettare la documentazione giuridica per renderla più comprensibile[18]. I contenuti vengono elaborati attraverso infografiche, animazioni, schemi visivi, mappe concettuali o strumenti interattivi, utilizzando la tecnologia e le competenze grafiche proprie del design.

Con una cautela essenziale: per design non deve intendersi solo l'aspetto esteriore, ma l'intero processo di progettazione.

Non si tratta di una semplice trasformazione del testo in immagine: bisogna assicurare che il significato originario e l'interpretazione finale coincidano. Ed è fondamentale evitare che la comunicazione venga equivocata o manipolata: anzi, il legal design deve contribuire proprio ad evitare fraintendimenti.

Per questo, i parametri da tenere in considerazione sono:

- il concetto che si vuole rappresentare;

18 *Hagan M., Law by design, https://lawbydesign.co*

- il modo in cui il simbolo che si vuole utilizzare (immagine, icona, ecc.) viene di norma percepito;
- il destinatario della comunicazione, ossia l'interpretante.

La convergenza tra competenze trasversali (legali, tecniche, grafiche, comunicative) rende possibile individuare il migliore strato tecnologico, ridisegnare le interfacce utente (user interfaces - UI) graficizzandone i contenuti, eliminando le informazioni sovrabbondanti, semplificando i testi e la visualizzazione, fino a coinvolgere il destinatario adottando anche le strategie della gamification.

IL RICORSO AL LEGAL DESIGN NELL'ACQUISIZIONE DEL CONSENSO INFORMATO AL TRATTAMENTO MEDICO

Utilizzare il legal design nell'acquisizione del consenso al trattamento – o meglio, già nel momento informativo propedeutico al consenso stesso – significa attrarre il paziente verso la lettura e la conoscenza effettiva dei contenuti dei moduli che riceve, e aiutarlo a capire i dettagli clinici della prestazione sanitaria.

Dettagli che altrimenti il paziente avrebbe rinunciato ad approfondire, sviluppando una sensazione di frustrazione, dovuta all'incomprensione, in grado di portarlo a richiedere un risarcimento anche in mancanza di un danno causalmente ascrivibile alla condotta del medico.

Rischio ulteriore, e ancor più frequente, è che l'assistito, insoddisfatto delle informazioni ricevute, ricorra a indicazioni, magari più chiare ma diffuse da fonti non autorevoli, accessibili soprattutto online.

Applicare il legal design in sanità significa creare un percorso che aiuti la persona assistita a comprendere i chiarimenti che gli vengono forniti, per consentirgli di esprimere, riguardo ai trattamenti medici, così come ai trattamenti che coinvolgono i suoi dati personali, una informed choice.

Obiettivo di questo approccio è progettare esperienze utente (user experience - UX) finalizzate a comunicare in modo corretto ed efficace le informazioni, anche con il supporto di tool aggiuntivi – come i biomodelli stampati in 3D che riproducono in scala

1:1 il distretto anatomico lesionato del paziente al massimo della sua verosimiglianza[19] – o tramite piattaforme digitali.

Il primo step, a livello operativo, consiste nell'identificare i punti di contatto (touchpoint) tra l'assistito e i processi e i documenti della struttura sanitaria, dalle pratiche di accettazione fino alle dimissioni del paziente.

Tradizionali touchpoint della customer journey in sanità sono:

L'informativa generale sul trattamento dei dati personali fornita in accettazione dalla struttura sanitaria;

- Le informative privacy relative a trattamenti specifici (ad es. con finalità di ricerca scientifica) sottoposte progressivamente;
- Gli eventuali moduli di consenso laddove il trattamento di dati si fondi su tale base giuridica;
- Il modulo contenente le spiegazioni sul trattamento medico e la manifestazione del consenso informato del paziente;

a cui possono eventualmente aggiungersi, ad esempio, la ricezione di reclami e il rilascio di feedback.

L'obiettivo è rivedere in chiave strategica questi passaggi, assicurando al paziente una piena consapevolezza del processo di cura.

Per questo è strategico individuare tramite gap analysis le carenze delle procedure aziendali nella gestione dei vari step, in un assessment continuo e circolare, e ricorrere al supporto che possono fornire i tool tipici del legal design, a partire da una indispensabile multidisciplinarietà.

L'incontro tra diverse competenze, infatti, è qui imprescindibile.

La necessaria conoscenza della normativa di riferimento, prerogativa di avvocati e consulenti legali, richiede il loro contributo per garantire che i contenuti giuridici siano conformi alle disposizioni di legge.

19 Bizzotto N. et al. Repliche anatomiche stampate in 3D: un nuovo strumento per la pianificazione chirurgica e il consenso informato, GIHTAD, 2017. 10:3

I medici possiedono, invece, le cognizioni scientifiche per illustrare i dettagli clinici esatti al paziente.

Per questo motivo, ai professionisti legali e sanitari spetta stabilire la sostanza dei contenuti dei moduli sottoposti ai pazienti.

I contenuti, ove opportuno, possono poi essere veicolati tramite la tecnologia più adatta allo scopo, coinvolgendo le competenze di web e graphic designers, content creators, UX e UI designers[20].

Il linguaggio da utilizzare deve essere riprogettato, anche con il contributo di esperti di comunicazione o psicologi, a fronte delle personas di riferimento (i pazienti) senza alterare o manipolare l'interpretazione del significato originario.

«Applicare il legal design in sanità significa creare un percorso che aiuti la persona assistita a comprendere i chiarimenti che gli vengono forniti, per consentirgli di esprimere, riguardo ai trattamenti medici, così come ai trattamenti che coinvolgono i suoi dati personali, una informed choice.»

Per evitarlo, i medici e professionisti legali sono tenuti a verificare che la correttezza dei contenuti e la compliance normativa nel processo e dei testi non siano state alterate.

In alcuni casi, poi, il reframing dei documenti legali può andare di pari passo con la scelta di accelerare la transizione verso il digitale – esigenza sempre più sentita nel settore medico – con una evidente ottimizzazione dei processi.

Si pensi a una delle maggiori criticità, affrontate sul piano amministrativo, delle strutture sanitarie: la crescente mole di cartaceo da archiviare. La carta non solo occupa spazio fisico, ma è esposta ad un rischio di violazione di dati che – a seconda delle vulnerabilità riscontrate in rapporto alle misure di sicurezza adottate ex art. 32 GDPR – può essere anche maggiore rispetto al rischio di cyber-attacco o di bug informatico.

---

20 Messori G. e Giacomello M. Legal Design: metodologia di assessment e reframing di documenti giuridici, in Martinelli S., Rossi Chauvenet C. Legal tech, contract re-design & big data per professionisti e imprese, Wolters Kluwer, 2022, pp. 480-501

La ragione della retention dei documenti in formato cartaceo è prevalentemente difensiva. L'interesse è conservare le firme autografe apposte dai pazienti sui moduli sopra citati in caso di contestazioni, in quanto le firme scansionate, prive di valore legale, non sarebbero sottoponibili a perizia grafologica.

La soluzione per digitalizzare a monte questo processo prevede l'acquisizione della firma grafometrica[21] degli assistiti attraverso l'uso di un tablet.

Introdurre una componente tecnologica può creare un'occasione per innovare l'interazione tra paziente e struttura utilizzando il device, ad esempio, anche per mostrare dei percorsi interattivi o simulazioni video che esplicitano le informazioni relative all'intervento medico.

«In mancanza di standard internazionali applicabili agli scenari di healthcare dei diversi Paesi che intervengano ad illustrare le modalità con cui perfezionare le abilità comunicative della classe medica, e come futuro supporto ad esse, il legal design può fin d'ora coinvolgere il paziente nel percorso terapeutico nel modo più rapido ed efficace.»

In ogni caso, la scelta finale sul tipo di grafica, di esperienza d'uso e di interfaccia[22] deve essere calibrata sulla tipologia di paziente e, lato struttura sanitaria, bilanciare le esigenze di budget.

L'impiego della tecnologia, inoltre, richiede un'integrazione con il rispetto degli artt. 25 e 32 del GDPR: fin dalla progettazione del trattamento dovranno essere adottate misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento sulla protezione dei dati.

---

21 La firma grafometrica rappresenta un dato biometrico ai sensi dell'art. 4, par. 1, n. 14) del GDPR in quanto è ottenuta da un trattamento tecnico specifico relativo alle caratteristiche fisiche di una persona fisica che ne consentono o confermano l'identificazione univoca

22 Giacomello M. Legal services: la creazione del prodotto in ambito legale, in Martinelli S., Rossi Chauvenet C. Legal tech, contract re-design & big data per professionisti e imprese, Wolters Kluwer, 2022, pp. 71-89

CONCLUSIONI

Centrando l'approccio sugli utenti del servizio sanitario, il legal design è in grado di trasformare gli adempimenti legali – a stento tollerati nel settore medico – in strumenti di empowerment dei pazienti e di fidelizzazione verso le strutture sanitarie e, più in generale, verso la sanità.

In mancanza di standard internazionali applicabili agli scenari di healthcare dei diversi Paesi che intervengano ad illustrare le modalità con cui perfezionare le abilità comunicative della classe medica, e come futuro supporto ad esse, il legal design può fin d'ora coinvolgere il paziente nel percorso terapeutico nel modo più rapido ed efficace.

Si tratta di un modello su cui basare anche il continuo potenziamento dell'e-health.

Se, infatti, l'obiettivo è fare in modo che le applicazioni digitali per la salute siano ampiamente utilizzate anche in contesti istituzionali, è necessario che godano della fiducia dei pazienti, della società e dei mercati. In questa sfida il legal design – realizzando prodotti e servizi user-centered – può fornire un apporto cruciale.

E se è vero che, come stabilisce la L. 219/2017, "il tempo della comunicazione tra medico e paziente costituisce tempo di cura", in termini di responsabilità sanitaria il costo della mancata chiarezza nelle informazioni può essere molto alto.

Superare il paradigma del "please sign here" è la chiave: il legal design è la metodologia che, per la prima volta nella storia, può contribuire a renderlo concretamente possibile.

LA REGOLAMENTAZIONE MICAR: UN'OCCASIONE PER SVILUPPARE NUOVE IDEE NEL MERCATO DELLE CRIPTO-ATTIVITÀ, GENERARE BENEFICI PER TUTTO IL SISTEMA FINANZIARIO E GARANTIRE LA SICUREZZA DELLE TRANSAZIONI

Alessandro Rodolfi, DataConSec

Al termine di una lunga consultazione pubblica iniziata in seno alla Commissione Europea nel dicembre del 2019, il 9 giugno 2023 il legislatore comunitario ha promulgato il Regolamento UE 2023/1114, noto come "MiCA Regulation" (MiCAR). L'obiettivo dell'UE è quello di creare un mercato unico digitale nel campo delle cripto-attività adottando regole comuni in tutti i Paesi europei al fine di evitare distorsioni e arbitraggi normativi. Inoltre l'Europa, da sempre molto attenta ai diritti dei suoi cittadini, ha voluto imporre maggiori tutele per limitare i rischi inerenti al fallimento degli exchange[1] e quelli generati dalle Initial Coin Offering (ICO) fraudolente verificatesi soprattutto nel biennio 2017-2018. Curioso notare invece come negli Stati Uniti, dove le criptovalute hanno visto la luce, la Securities and Exchange Commission (SEC) guidata da Gary Gansler stia ostacolando duramente la regolamentazione, attraverso cause legali avviate nei confronti dei maggiori operatori americani.

L'applicazione del MiCAR, pur essendo prevista in due differenti step a partire dalla seconda metà del 2024, vede l'Europa all'avanguardia nella creazione del primo framework

1 *Nel momento in cui sto scrivendo si sta svolgendo il processo per il fallimento di FTX, uno degli exchange più grandi del mondo, che vede coinvolto tra gli altri il suo ex CEO e fondatore Sam Bankman-Fried. La bancarotta, che ha coinvolto fino a 1 milione di risparmiatori per un importo stimato di 30 miliardi di dollari, ha avuto delle ripercussioni devastanti per tutto il mondo crypto.*

legislativo al mondo che ha l'ambizione di normare in maniera omogenea una materia così complessa, che pone le sue basi su un'innovazione tecnologica vertiginosa in costante e rapida evoluzione. Pur non essendo questa la sede opportuna per entrare nel merito delle singole previsioni contenute nel Regolamento, è importante notare come queste riguardino sia gli emittenti di criptovalute e token (soprattutto stablecoin[2]), sia i "Crypto Asset Service Provider" (c.d CASP)[3]. Tali soggetti, potendo contare su "regole del gioco" chiare sulla correttezza della loro operatività, saranno sicuramente più propensi a effettuare investimenti nel Vecchio Continente creando una notevole crescita per l'industria crypto e indirettamente anche per tutti i settori che ne saranno contaminati, FinTech in primis.

«L'applicazione del MiCAR, pur essendo prevista in due differenti step a partire dalla seconda metà del 2024, vede l'Europa all'avanguardia nella creazione del primo framework legislativo al mondo che ha l'ambizione di normare in maniera omogenea una materia così complessa, che pone le sue basi su un'innovazione tecnologica vertiginosa in costante e rapida evoluzione.»

Il percorso per cogliere tali opportunità è dunque solo all'inizio e i suoi effetti potrebbero avere un impatto dirompente sul funzionamento dei pagamenti digitali, sulla tutela dei risparmiatori, degli investitori e in generale sulla stabilità dell'intero sistema finanziario. Anche per queste motivazioni la Banca d'Italia, già nel quadro della sperimentazione

2 Le stablecoin sono un tipo di criptovalute che riproducono il valore di una valuta quale per esempio l'euro o il dollaro americano (c.d valute fiat) attraverso un meccanismo di ancoraggio (pegging) che permette di contrastare la volatilità tipica delle criptovalute.

3 I CASP sono dei prestatori di servizi e intermediari attivi nel campo delle cripto-attività, che si occupano per esempio di custodia e amministrazione di cripto-attività per conto di clienti, della gestione di piattaforme di negoziazione di cripto-attività, scambio di cripto-attività con fondi, scambio di cripto-attività con altre cripto-attività, ricezione e trasmissione di ordini di cripto-attività per conto di clienti, prestazione di consulenza sulle cripto-attività, prestazione di gestione di portafoglio sulle cripto-attività.

prevista dal DLT Pilot Regime[4], si è fatta promotrice di una serie di iniziative[5] al fine di sostenere la crescita di operatori innovativi nell'applicazione della tecnologia DLT che siano in grado di sviluppare buone pratiche nel rispetto dei principi di sicurezza, inclusione, trasparenza, sostenibilità ed efficienza. In particolare, i due ambiti in cui si stanno concentrando maggiormente le sperimentazioni sono la tokenizzazione di asset tradizionali attraverso DLT o blockchain[6] e le stablecoin. Quest'ultime stanno assumendo sempre più importanza: la più grande stablecoin sul mercato per capitalizzazione, Tether (USDT) agganciata al dollaro USA in modo che a 1 USD₮ corrisponda 1 USD, al 30 giugno 2023 ha dichiarato asset totali per più di 86 miliardi di dollari. Come si può osservare sia la tokenizzazione che le stablecoin sono entrambi connessi agli asset presenti nel "mondo reale" (bond, azioni, valute fiat, ecc.) in modo da rendere il graduale passaggio, affatto banale, tra la finanza tradizionale e quella decentralizzata.

«In via indiretta inoltre saranno sempre più necessarie risorse e professionalità legate allo sviluppo di codice sicuro (soprattutto per il Web 3 e gli smart contract), alla compliance con le nuove regolamentazioni, alla cybersecurity e all'auditing per la verifica delle vulnerabilità delle piattaforme digitali e, ultima ma non meno importante, alla formazione sulle opportunità e i rischi delle cripto-attività.»

In tal senso tra i progetti più significativi ammessi dalla Banca d'Italia nell'ambito della Call for proposals 2022 di Milano HUB si segnalano:

- Lo sviluppo di una piattaforma di tokenizzazione di Titoli di Stato regolati tramite

4 Il DLT Pilot regime, introdotto con Regolamento UE 2022/858, norma attraverso un regime temporaneo e sperimentale l'emissione e la circolazione degli strumenti finanziari in forma digitale al fine di permettere di testare i servizi finanziari attraverso l'utilizzo della DLT.

5 Call for proposals 2022 di Milano HUB negli ambiti FinTech Hub, Innovation Hub e Research and Development Hub.

6 Da sottolineare l'attuale tendenza dei "Real World Asset" (RWA) che permette la tokenizzazione degli asset esistenti nella finanza tradizionale.

smart contracts[7];

- La creazione di una piattaforma per la sperimentazione della DeFi istituzionale, attraverso i security token[8];
- Tecnologie a supporto della "Prova di Riserva Individuale", che permette agli utenti di verificare in modo autonomo le proprie cripto-attività detenute in custodia presso gli intermediari[9];
- Costituzione di uno standard di e-money token interoperabili emessi da banche e circolanti su tecnologia blockchain (stablecoin)[10];
- Decentralizzazione della verifica dell'identità digitale (KYC) attraverso un sistema decentralizzato e più sicuro per il Web 3[11];
- Lo sviluppo di una piattaforma per l'emissione di strumenti di debito tokenizzati su blockchain pubblica con l'obiettivo di finanziare le PMI italiane[12];
- Emissione di un e-money token al fine di esaminare, validare e testare l'architettura tecnologica di una stablecoin[13];
- Digitalizzazione dei processi M&A su blockchain, al fine di ottimizzare la gestione amministrativa di quote partecipative[14];
- Lo sviluppo di una piattaforma condivisa basata su DLT che permetta l'associazione dei dati di un asset immobiliare con quelli del mutuo per fini legati alle garanzie bancarie[15];

7 *Algorand Labs S.r.l.*

8 *Cetif Advisory*

9 *CheckSig S.r.l.*

10 *Conio S.r.l.*

11 *Cyberneid S.r.l.*

12 *Real House S.r.l.*

13 *Banca Sella Holding*

14 *Credem Euromobiliare Private Banking S.p.A.*

15 *Associazione Blockchain Italia*

- Realizzazione di uno strumento di governance basato su blockchain per la gestione dei fondi (DAO)[16].

Tra gli scenari futuri dell'industria crypto ipotizzati da Brian Armstrong, co-fondatore di Coinbase[17] e personaggio di spicco del settore, si segnalano: le criptovalute che permettono di proteggersi dall'inflazione[18], la gestione della reputazione on-chain, la gestione della pubblicità on-chain, lo sviluppo di Layer 2 orientati alla privacy e lo sviluppo del Web3 in relazione al gaming anche attraverso l'utilizzo degli NFT.

In via indiretta inoltre saranno sempre più necessarie risorse e professionalità legate allo sviluppo di codice sicuro (soprattutto per il Web 3 e gli smart contract), alla compliance con le nuove regolamentazioni, alla cybersecurity e all'auditing per la verifica delle vulnerabilità delle piattaforme digitali e, ultima ma non meno importante, alla formazione sulle opportunità e i rischi delle cripto-attività.

L'Europa, giocando d'anticipo sugli altri regolatori mondiali, potrebbe creare un mercato crypto di altissimo valore e attrarre molti capitali anche da organizzazioni extra UE, sfruttando quello che viene definito il "Brussels effect", ovvero il fenomeno per cui le organizzazioni finiscono per conformarsi alle norme dell'UE anche al di fuori dei suoi confini per motivi legati prevalentemente alla compliance. Si tratta indubbiamente di un'opportunità formidabile per l'avvio di nuovi business anche nel campo del Legal Tech.

---

16 Politecnico di Milano

17 Società leader nel settore delle criptovalute (prima del settore a essere quotata al NASDAQ)

18 Flatcoin

METAVERSO: NUOVA FRONTIERA DELL'INFLUENCER MARKETING

Giulia Suigo e Riccardo Lanzo, Lanzo & Partners

IL MERCATO DELL'INFLUENCER MARKETING

Dalla pubblicità tradizionale e generalizzata si sta passando a quella targettizzata e integrata, in cui il digital si fa sempre più spazio.

Stiamo assistendo a un fenomeno globale economicamente, socialmente e giuridicamente rilevante, che sta rivoluzionando i rapporti tra i consumatori e le imprese, grazie all'ascesa degli influencer, figure che si evolvono con il mutare delle dinamiche sociali ed economiche e che rispondono, a diversi livelli, alle domande del mercato, rappresentando il touchpoint in grado di attivare i propri follower, avendo un rapporto diretto e di fiducia con la propria community[1].

L'influencer marketing è un'ormai consolidata modalità di comunicazione, consistente nella "diffusione su blog, vlog e social network di foto, video e commenti da parte di blogger e influencer che mostrano sostegno o approvazione (endorsement) per determinati brand, generando un effetto pubblicitario."[2]

Guardando i numeri, il mercato globale dell'influencer marketing registra una crescita continua e da record. Le sue dimensioni sono più che raddoppiate, passando da 6.5 miliardi di dollari nel 2019 a 16.4 miliardi di dollari nel 2022, e si stima che nel 2023 raggiungerà

1 *R. Lanzo e M. Giordano, Il diritto degli influencer, p. 12, disponibile al seguente link: https://42talent.it/*

2 *AGCM, 25 febbraio 2020, n. 28167*

21,1 miliardi di dollari.[3]

Anche il mercato italiano – registrando nel 2021 volumi di circa 280 milioni di euro (+15% rispetto al 2020) e raggiungendo, nel 2022, 308 milioni di euro (+10% rispetto al 2021) – mostra una crescita destinata a non fermarsi, sebbene inferiore rispetto al trend internazionale. Secondo le stime di DeRev, infatti, nel 2023 si potrebbe registrare un giro d'affari pari a 348 milioni di euro (+13% rispetto al 2022). Quest'anno, i settori trainanti si confermano essere Fashion & Beauty (25% del mercato) Gaming (12,9%) e Travel & Lifestyle (12,5%).[4]

«Guardando i numeri, il mercato globale dell'influencer marketing registra una crescita continua e da record. Le sue dimensioni sono più che raddoppiate, passando da 6.5 miliardi di dollari nel 2019 a 16.4 miliardi di dollari nel 2022, e si stima che nel 2023 raggiungerà 21,1 miliardi di dollari.»

L'APPRODO DELL'INFLUENCER MARKETING NEL METAVERSO E L'ASCESA DEI VIRTUAL INFLUENCER

L'influencer marketing, essendo un fenomeno dinamico, è approdato al metaverso[5], anzi, ai metaversi, che rappresentano dei veri e propri mondi paralleli e virtuali. [6]

Per semplicità espositiva, nel prosieguo si farà riferimento al metaverso intendendolo come "insieme di ambienti virtuali tridimensionali in cui le persone possono interagire

3 V. Dencheva, Global influencer marketing value 2016-2023, 10.05.2023, disponibile al seguente link https://www.statista.com/statistics/1092819/global-influencer-market-size/

4 Compensi degli influencer in Italia: il listino 2023 di DeRev, 05.07.2023, disponibile al seguente link https://derev.com/2023/07/compensi-degli-influencer-2023-listino/

5 Termine apparso per la prima volta in Neal Stephenson, Snow Crash, Publisher: Bantam Books, New York, 1992, per far riferimento ad un tipo di esperienza virtuale fortemente immersiva

6 Ad esempio, Decentraland, The Sandbox, Stageverse e Roblox.

tra loro attraverso avatar personalizzati”[7] caratterizzato da assenza di confini geografici, che rappresenta il trait d’union tra la realtà virtuale e quella fisica, permettendo di avere, rispetto ai social network, interazioni più simili a quelle reali grazie alle sue caratteristiche peculiari, quali l’effimerità e l’immersività.

Il metaverso è popolato da avatar, che si muovono in un ambiente comune, spesso simile al mondo reale, in cui vivono esperienze ed interagiscono tra loro.

Ciascun avatar può essere sia l’alter ego di una determinata persona, di cui solitamente riporta le sembianze, sia frutto esclusivo dell’immaginazione di chi lo ha creato ad hoc per abitare il metaverso, senza che rappresenti, quindi, la trasposizione di alcuna persona fisica esistente nel mondo reale.

Negli ultimi anni, alcuni brand, intuendo le immense opportunità di questo nuovo mondo, hanno iniziato a convogliare parte delle proprie attività di marketing nel metaverso sviluppando anche progetti di influencer marketing.

«Ad oggi, non esiste una normativa ad hoc riferita al mondo virtuale: gli interpreti devono riferirsi a un quadro normativo frammentario e statico, che ontologicamente non tiene il passo con il dinamismo tipico del mondo digitale.»

Se sui social network ci sono gli influencer, nel metaverso troviamo i virtual influencer, avatar addetti a sponsorizzare importanti marchi sbarcati nel mondo virtuale. Possono essere definiti “influencer perfetti” dal punto di vista del marketing, poiché studiati e realizzati in base alla community che andranno ad interessare, potendo anche diventare portavoce di battaglie civili e sociali particolarmente attuali.[8] L’attività dei virtual influencer non si arresta nel metaverso: posseggono anche profili social in cui vengono

---

7 Accademia della Crusca, definizione disponibile al seguente link https://accademiadellacrusca.it/it/parole-nuove/metaverso/21513 ; definito anche “zona di convergenza di spazi virtuali interattivi, localizzata nel cyberspazio e accessibile dagli utenti attraverso un avatar con funzione di rappresentante dell’identità individuale” in G. Cassano, M. Iaselli e G. Spangher, Cybersicurezza e sicurezza nazionale nel Metaverso, in AA.VV., Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d’autore – profili penali – blockchain e NFT, a cura di G. Cassano e G. Scorza, Pisa: Pacini Editore S.r.l., 2023

8 R. Lanzo, L’influencer marketing nell’era del Metaverso, ibidem

pubblicati contenuti che rappresentano momenti della loro vita digitale, proprio come gli influencer in carne ed ossa. [9]

Ma il fenomeno non si arresta qui. Sono stati creati ex novo anche virtual brand ambassador che riflettono e si fanno portavoce dei valori del marchio che rappresentano. [10]

IL QUADRO NORMATIVO

Ad oggi, non esiste una normativa ad hoc riferita al mondo virtuale: gli interpreti devono riferirsi a un quadro normativo frammentario e statico, che ontologicamente non tiene il passo con il dinamismo tipico del mondo digitale.

Focalizzandosi sull'influencer marketing nel metaverso, si tratta principalmente di comprendere come applicare le norme in tema di marchi, pubblicità, diritto d'autore e diritti di immagine.

Per quanto attiene alla tutela dei marchi nel metaverso, dal 2021 si è sviluppata la prassi lungimirante, recepita dalla dodicesima edizione della Classificazione di Nizza del 2023, di depositare domande di registrazione con espresso riferimento, ad esempio, a "beni virtuali scaricabili inclusi gli NFTs", "negozi al dettaglio di beni virtuali" e "servizi di intrattenimento in ambienti virtuali". [11]

Con riferimento alla contraffazione, in base alle policy in materia di tutela dei diritti IP del metaverso di riferimento, accettate da tutti gli utenti, la rimozione dei prodotti virtuali contraffatti diviene più semplice.

Ebbene, quando i prodotti vengono pubblicizzati all'interno del metaverso, trovano

9 Tra i virtual influencer più conosciuti a livello mondiale si annoverano Noonoouri, che è parte del roster di IMG Models e ha rappresentato brand come Versace, Gucci, Fendi e Roberto Cavalli; Lil Miquela, che conta quasi 3 milioni di follower su Instagram e promuove brand del calibro di Samsung, Calvin Klein e UGG e sostiene il movimento "Black Lives Matter"; Lu Do Magalu, che conta oltre 6 milioni di follower su Instagram e 2,75 milioni di iscritti al proprio canale YouTube; Zaira, la prima virtual influencer italiana, portavoce dei valori della generazione Z: body positivity, sostenibilità ambientale, inclusione e consapevolezza.

10 Ad esempio, Daisy impersona le posizioni di Yoox sulla sostenibilità e sulle questioni sociali e Candy promuove la medesima fragranza di Prada e indossa gli accessori iconici della maison

11 Rientranti, rispettivamente, nelle classi 9, 35 e 41 della Classificazione internazionale di Nizza. Ad esempio, il marchio denominativo europeo "Nike" (domanda n. 018586666), il marchio denominativo francese "Balenciaga" (domanda n. 4837618) e il marchio denominativo europeo "Gucci" (domanda n. 018717545)

applicazione le disposizioni di cui al Codice del Consumo in tema di pratiche commerciali scorrette e la soft law rappresentata dal Codice di Autodisciplina della Comunicazione Commerciale, Regolamento Digital Chart incluso, emanato dallo IAP. In particolare, il Regolamento Digital Chart, all'art. 2 "Endorsement", chiarisce che trova applicazione anche nei confronti di quelli che potremmo chiamare, con un neologismo, "virtual influencer nativi", stabilendo che "nel caso in cui l'accreditamento di un prodotto o di un brand, posto in essere da celebrity, influencer, blogger, o altre figure simili di utilizzatori della rete che con il proprio intervento possano potenzialmente influenzare le scelte commerciali del pubblico, (di seguito, collettivamente, "influencer"), siano essi umani o virtuali, abbia natura di comunicazione commerciale, deve essere inserita in modo ben visibile nella parte iniziale del post o di altra comunicazione diffusa in rete una delle seguenti diciture: "Pubblicità/Advertising", o "Promosso da… brand/Promoted by… brand" o "Sponsorizzato da… brand/Sponsored by… brand", o "In collaborazione con… brand/In partnership with… brand". Ciò con riferimento ad attività di influencer marketing svolte sia nel metaverso sia attraverso i social network.

Tali iniziative pubblicitarie, poi, potendo coinvolgere sia virtual influencer nativi che avatar che rappresentano l'alter ego di influencer, richiedono la sottoscrizione di contratti aventi contenuto parzialmente diverso. Infatti, nel primo caso, il contratto dovrà contenere la licenza di utilizzazione economica dell'opera costituita dall'avatar stesso concessa dal suo creatore o da chi ne detiene i diritti, invece, nel secondo caso, l'influencer dovrà anche concedere in licenza il diritto di sfruttare economicamente la propria immagine.

A ciò si aggiunga il doveroso rispetto delle norme poste a tutela della leale concorrenza e delle policy del metaverso di riferimento.

Si consideri, infine, che anche nel metaverso, la contraffazione di marchi e il plagio di opere comportano anche il risarcimento dei danni patiti dai legittimi titolari dei diritti violati e, in alcuni casi, assumono anche rilevanza penale.

Da approfondire, caso per caso, saranno il diritto applicabile e, in caso di contenzioso, la competenza giurisdizionale.

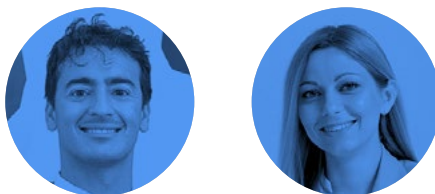
CONCLUSIONI

Appare evidente che la pubblicità diventerà sempre più invasiva ed immersiva e troverà nel metaverso terreno fertile in cui fiorire. L'influencer marketing riferito al metaverso rappresenta, oggi, la nuova frontiera per aumentare notorietà e profitti derivanti dallo sfruttamento economico dei brand e degli influencer.

Nello specifico, il coinvolgimento di virtual influencer nativi può annullare il rischio di danni reputazionali ed i costi relativi agli spostamenti degli influencer tradizionali, ferma restando la necessità di prestare la massima attenzione, nella negoziazione dei contratti di endorsement e ambassadorship, a tutti i temi accennati, senza tralasciare, inoltre, privacy e cybersecurity.

Ci si auspica, infine, un intervento tempestivo e puntuale da parte del legislatore che detti una disciplina organica del cyberspazio a tutela dei diritti di tutti i soggetti coinvolti, utenti, influencer e brand, al fine di evitare usi distorti e lesivi delle iniziative di influencer marketing relative al metaverso.

I NUOVI ORIENTAMENTI DELL'UNIONE EUROPEA SULLA RESPONSABILITÀ PER I DANNI DA INTELLIGENZA ARTIFICIALE

Luca Tormen e Marianna Riedo, Portolano Cavallo

Nel 2023 sono stati fatti sostanziali passi avanti nella disciplina dell'intelligenza artificiale (IA). Il protagonista del dibattito è stato senz'altro il regolamento denominato "AI Act"[1], che definirà i principi che regolano l'utilizzo dell'IA. Questo, in estrema sintesi[2], propone un approccio modulato sul rischio:

- I sistemi che pongono un rischio inaccettabile[3] data la minaccia che rappresentano per le persone saranno vietati;

1 Ad oggi (20 dicembre 2023), il testo dell'AI Act non è ancora definitivo. Nonostante il Parlamento europeo e la Presidenza del Consiglio UE abbiano raggiunto un accordo provvisorio sulla proposta lo scorso 9 dicembre, il testo della legge necessita ancora di essere messo e punto e rivisto per assicurarne la correttezza sotto il profilo tecnico. Si stima che una versione definitiva del testo verrà diffusa e sottoposta ad approvazione a inizio 2024. Nel frattempo, è possibile consultare online la proposta di regolamento pubblicata dalla Commissione europea il 21 aprile 2021 (disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206) e gli emendamenti approvati dal Parlamento europeo a giugno 2023, (disponibili al link: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html). La Commissione europea ha inoltre reso disponibile un documento di Q&A aggiornato a seguito dell'accordo raggiunto il 9 dicembre 2023 (disponibile al link: https://ec.europa.eu/commission/presscorner/detail/it/QANDA_21_1683).

2 Per una panoramica più completa sulla strategia dell'Unione europea in materia di intelligenza artificiale, si rimanda alla pagina dedicata sui siti della Commissione europea (https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence) e del Parlamento europeo (https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence).

3 Le pratiche vietate, elencate anche nel documento di Q&A pubblicato dalla Commissione europea a dicembre 2023 (cfr. supra, nota 1) includono, ad esempio, i sistemi che pongono il rischio di attuare discriminazioni tramite l'utilizzo di sistemi di punteggio sociale o polizia predittiva, quelli basati sull'identificazione biometrica in tempo reale in spazi accessibili al pubblico o quelli che comportano il rischio di uno sfruttamento della vulnerabilità delle persona attraverso l'utilizzo di tecniche subliminali.

- I sistemi ad alto rischio di influire negativamente sulla sicurezza o sui diritti fondamentali[4] saranno soggetti a obblighi rigorosi;
- I sistemi a basso rischio potranno essere sviluppati e utilizzati nel rispetto della legislazione vigente, senza ulteriori obblighi giuridici;
- Alcuni sistemi capaci di porre rischi specifici per la trasparenza[5] saranno vincolati da limiti meno stringenti, mirati a garantire adeguata chiarezza sul funzionamento del sistema e, di conseguenza, la decisione informata.

Il regolamento mira a ridurre i rischi per i diritti fondamentali, la salute e la sicurezza, ma non disciplina specificamente le conseguenze negative che derivano dall'IA.

LA DIRETTIVA SULLA RESPONSABILITÀ DA IA

Per colmare il presunto[6] vuoto normativo, la Commissione europea ha emesso una proposta di direttiva sull'adeguamento della disciplina della responsabilità extracontrattuale all'intelligenza artificiale (la "Direttiva sulla responsabilità da IA")[7].

---

4 L'Allegato III dell'AI Act (dato aggiornato al 20 dicembre 2023) fornisce un elenco di casi d'uso ritenuti ad alto rischio, che la Commissione provvederà a mantenere aggiornato e in linea con l'evoluzione della tecnologia. Questi includono, tra gli altri, i sistemi di gestione di infrastrutture critiche, gestione dei lavoratori, accesso a servizi privati essenziali, controllo delle frontiere e così via. Questi sistemi dovranno essere registrati in un'apposita banca dati e saranno oggetto di costante valutazione. Secondo le stime formulate dalla Commissione europea in sede di stesura della prima bozza dell'AI Act, le soluzioni di IA destinate a rientrare nella categoria di sistemi ad alto rischio si aggirano intorno al 5-15% del totale. Sarà possibile effettuare una stima più precisa solo a seguito della lettura del testo definitivo dell'AI Act.

5 Possono rientrarvi, ad esempio, i sistemi che manipolano contenuti di immagini, audio o video (es. deepfake): all'attuale stato dell'arte (ma i problemi che il fenomeno sta ponendo potrebbero portare a un cambio di rotta) questi non sarebbero vietati, ma andrebbe reso noto l'utilizzo dell'IA nella loro creazione.

6 Tra i giuristi vi è chi ritiene che le norme vigenti, per la loro elasticità, siano già sufficienti a disciplinare il regime di responsabilità dei sistemi di IA. Un approfondimento di questa prospettiva sarebbe sovrabbondante in questa sede. Si ritiene sufficiente rendere noto che, a supporto di questa argomentazione, si cita, per esempio, la capacità di molte norme di origine romana e tuttora applicate di sopravvivere ai vari stravolgimenti industriali. v. G. Romano, Diritto, robotica e teoria dei giochi: riflessioni su una sinergia, in G. Alpa (a cura di), Diritto e intelligenza artificiale, Pacini Giuridica, 2022, 103 ss.

7 Il testo della proposta pubblicato dalla Commissione europea è disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0496.

La premessa è che le attuali regole sulla responsabilità civile, e specie quelle interne fondate sul criterio della colpa, sono ritenute inadeguate a risarcire i danni causati dall'IA[8].

Spesso, in base a queste norme, le parti lese hanno l'obbligo di dimostrare, tra l'altro, la negligenza, l'imperizia o l'imprudenza a causa del danno. Ma le caratteristiche qualitative specifiche dell'IA, prime tra tutte la sofisticatezza tecnica e l'autonomia dei sistemi nella produzione del risultato, rendono particolarmente complesso e talvolta impossibile l'adempimento di questo onere probatorio.

La proposta di Direttiva sulla responsabilità da IA propone allora di introdurre un regime di responsabilità sempre basato sulla colpa, ma che che allevi ulteriormente l'onere probatorio a carico dell'utente. Legata a doppio filo all'AI Act, al quale fa espresso rimando per aspetti fondamentali (tra cui la definizione stessa di intelligenza artificiale), la bozza prevede norme comuni a livello europeo sotto due principali aspetti: (a) le modalità di raccolta di elementi di prova sul funzionamento dei sistemi di IA ad alto rischio; e (b) l'onere della prova.

«Pur applicando le tradizionali regole di responsabilità oggettiva della direttiva sui prodotti di IA difettosi, la nuova proposta di direttiva fa un ulteriore passo avanti verso un regime più rigoroso, introducendo una presunzione sul difetto di un prodotto o sul nesso di causalità tra il danno e il difetto.»

In relazione al primo punto, la proposta conferisce ai tribunali nazionali il potere di ordinare a fornitori o utilizzatori di sistemi di IA ad alto rischio di fornire ai soggetti lesi informazioni relative al funzionamento del sistema stesso, limitatamente a quanto necessario e proporzionato (tenendo conto degli eventuali segreti commerciali e di altre informazioni sensibili) a sostanziare le richieste di risarcimento dei soggetti lesi. Benché questa proposta non rappresenti una vera e propria inversione dell'onere della prova, con essa la Commissione intende agevolare i soggetti lesi nell'individuare i soggetti responsabili, nel

8 Si è optato per lo strumento della direttiva per garantire da un lato l'armonizzazione e la certezza del diritto auspicati, dall'altro la flessibilità necessaria per consentire agli Stati membri di integrare senza attriti le misure armonizzate nei rispettivi regimi nazionali di responsabilità.

chiarire il funzionamento del sistema e nell'identificare il passaggio che ha determinato il verificarsi del danno.

Quanto al secondo punto, la Direttiva sulla responsabilità da IA introduce[9] una "presunzione relativa di causalità", che alleggerisce l'onere della prova a carico dell'attore quando sono soddisfatte contemporaneamente le seguenti condizioni: (i) sia dimostrato che il convenuto non ha rispettato un obbligo di diligenza volto a proteggere dal danno che si è verificato, compresa l'inosservanza degli obblighi previsti dall'AI Act; (ii) si può ritenere "ragionevolmente probabile", in base alle circostanze del caso, che il mancato rispetto dell'obbligo abbia influenzato l'output prodotto dal sistema di IA o la sua mancata produzione; e (iii) sia dimostrato che l'output del sistema di IA o la sua mancata produzione ha causato il danno.

Il regime è ancor più rigido verso i sistemi di IA ad alto rischio (come definiti nell'AI Act[10]): i tribunali nazionali dovranno in ogni caso presumere il nesso di causalità tra la mancata osservanza dei requisiti previsti dall'AI Act e l'output prodotto dal sistema di IA o l'incapacità del sistema di IA di produrre un output che abbia causato un danno rilevante.

L'attuale bozza è stata assegnata alla revisione della commissione giuridica del Parlamento europeo (JURI). È probabile che le discussioni relative agli emendamenti prenderanno avvio solo nel corso del 2024, essendo stata fino ad oggi priorità delle istituzioni europee trovare un accordo sul testo dell'AI Act, la cui approvazione costituisce un presupposto essenziale per l'elaborazione e applicazione della Direttiva sulla responsabilità da IA.

LA PROPOSTA DI REVISIONE DELLA DIRETTIVA SULLA RESPONSABILITÀ PER DANNO DA PRODOTTI DIFETTOSI

Anche la proposta di una nuova Direttiva sulla responsabilità per danno da prodotti difettosi (la "Proposta di revisione della direttiva 85/374/CEE")[11] potrebbe avere un impatto sul regime dell'IA e, presumibilmente, fornire un terreno fertile per intentare azioni legali di

---

9 *Articolo 4 della proposta di direttiva formulata dalla Commissione.*

10 *Cfr. supra, nota 4.*

11 *Il testo della proposta pubblicato dalla Commissione europea è disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0495.*

potenziale notevole profilo. Questa condivide con la Direttiva sulla responsabilità da IA l'obiettivo di aggiornare e perfezionare le norme in materia di responsabilità civile in un mondo tecnologicamente avanzato.

Più specificamente, la nuova direttiva punta a sostituire la Direttiva 85/374/CEE ("Direttiva sulla responsabilità per danno da prodotti difettosi") con un quadro aggiornato che possa rispondere in modo più efficace alle esigenze dell'economia digitale. La Direttiva 85/374/CEE, che ha rappresentato una delle pietre miliari nel quadro giuridico del mercato unico europeo fin dagli anni '80, prevede nel caso di danno da prodotto difettoso un regime di responsabilità oggettiva (rectius, presunta) che consente al consumatore di ottenere il risarcimento in maniera particolarmente agevole. Ora, la revisione della direttiva mira a modernizzare la precedente normativa, inserendo una regolamentazione specifica dei software e dei prodotti digitali, includendo anche i prodotti dotati di IA nell'ambito di applicazione del regime di responsabilità per danni da prodotti difettosi.

«Ecco perché la Commissione europea è intervenuta con un doppio approccio per garantire che, oltre alla sicurezza e alla protezione dei diritti fondamentali legati all'IA (garantite dall'AI Act), sia offerta una protezione anche sul profilo risarcitorio, optando a seconda dei casi per un regime di responsabilità per colpa, presunta o oggettiva.»

Pur applicando le tradizionali regole di responsabilità oggettiva della direttiva sui prodotti di IA difettosi, la nuova proposta di direttiva fa un ulteriore passo avanti verso un regime più rigoroso, introducendo una presunzione sul difetto di un prodotto o sul nesso di causalità tra il danno e il difetto. La bozza[12] prevede infatti che se un tribunale nazionale stabilisce che la complessità tecnica o scientifica di un prodotto rende eccessivamente difficile per i danneggiati provare la sua difettosità o il nesso di causalità tra il difetto e il danno, tale difettosità o causalità può essere presunta.

Come meglio spiegato nel considerando n. 34 della nuova proposta di direttiva, in una

12 *Articolo 9 dell'attuale testo (dato aggiornato al 20 dicembre 2023).*

controversia relativa a un sistema di intelligenza artificiale, il danneggiato “non dovrebbe essere tenuto, affinché l’organo giurisdizionale possa accertare l’esistenza di difficoltà eccessive, a spiegare le caratteristiche specifiche di tale sistema di IA o il modo in cui tali caratteristiche complicano la prova del nesso di causalità. Il convenuto dovrebbe avere la possibilità di contestare l’esistenza di difficoltà eccessive”[13].

A seguito dell’adozione delle rispettive posizioni negoziali, il Consiglio dell’Unione europea[14] e il Parlamento europeo[15] hanno raggiunto un accordo preliminare il 14 dicembre 2023. Ad oggi[16], in attesa dell’adozione da parte della Plenaria, non è ancora stato diffuso il testo ufficiale della nuova legge.

CONCLUSIONI: PERCHÉ DUE DIRETTIVE?

Sorge spontaneo chiedersi se fosse realmente necessario affrontare il tema della responsabilità per danni derivanti dall'intelligenza artificiale con due direttive diverse.

L’UE rivendica la scelta sostenendo che entrambe le due proposte, insieme all’AI Act, siano essenziali per creare le giuste premesse per uno sviluppo sostenibile di prodotti e servizi dotati di intelligenza artificiale.

In particolare, ad oggi, la Direttiva sulla responsabilità per danno da prodotti difettosi e le disposizioni nazionali in materia di responsabilità civile prevedono azioni di responsabilità fondate su basi giuridiche diverse, nei confronti di soggetti responsabili diversi e per tipologie di lesioni e di danni diverse. Di conseguenza, queste norme si rivolgono a vari mercati e soggetti. Allo stato attuale, la Direttiva sulla responsabilità per danno da prodotti difettosi potrebbe applicarsi solo a una parte dei danni che possono essere causati dall’IA:

13 Il Parlamento europeo, negli emendamenti formulati in relazione al Considerando n. 34, a partire dalla proposta della Commissione, ha ulteriormente chiarito che “Il convenuto dovrebbe avere la possibilità di contestare l'esistenza di difficoltà eccessive, ad esempio dimostrando che l'attore dispone di elementi sufficienti per provare il carattere difettoso del prodotto o il nesso di causalità tra difetto e danno, o entrambi. In tal caso, non dovrebbero essere presunti il carattere difettoso di un prodotto o il nesso di causalità tra danno e difetto, o entrambi.”

14 Per ulteriori informazioni, si rimanda al link: https://www.consilium.europa.eu/en/press/press-releases/2023/06/14/the-council-adopts-its-negotiating-mandate-for-a-new-eu-law-on-liability-for-defective-products/.

15 Il testo della relazione del Parlamento europeo è disponibile al seguente link: https://www.europarl.europa.eu/doceo/document/A-9-2023-0291_IT.html.

16 20 dicembre 2023.

essa, per esempio, non copre i danni causati ai beni destinati all'uso professionale, i danni causati durante la fornitura di un servizio, i danni a vittime diverse dalle persone fisiche o le richieste di risarcimento derivanti dall'uso improprio di un prodotto. Ancora, la Direttiva sulla responsabilità per danno da prodotti difettosi individua il produttore quale soggetto responsabile, ma non copre i danni causati da altri soggetti come, ad esempio, i programmatori. In tutti questi casi, la tutela residuale dei soggetti danneggiati è garantita solo dalle normative interne.

Ecco perché la Commissione europea è intervenuta con un doppio approccio per garantire che, oltre alla sicurezza e alla protezione dei diritti fondamentali legati all'IA (garantite dall'AI Act), sia offerta una protezione anche sul profilo risarcitorio, optando a seconda dei casi per un regime di responsabilità per colpa, presunta o oggettiva.

«Insieme, le due proposte mirano a garantire il funzionamento del mercato interno dei prodotti e servizi abilitati all'IA e ad assicurare che le vittime di danni causati dall'IA abbiano lo stesso livello di protezione delle vittime di danni causati da altre tecnologie.»

Da un lato, la revisione della Direttiva sulla responsabilità per danno da prodotti difettosi mira ad adattare la legge all'era digitale, preservando però la neutralità tecnologica che ha sempre caratterizzato la sua applicazione. Inoltre, contribuisce a rendere più agevole la richiesta di risarcimento da parte delle vittime di danni causati da prodotti dotati di IA. Dall'altro lato, la Direttiva sulla responsabilità da IA risponde a problematiche specifiche poste dall'IA in materia di responsabilità extracontrattuale. Insieme, le due proposte mirano a garantire il funzionamento del mercato interno dei prodotti e servizi abilitati all'IA e ad assicurare che le vittime di danni causati dall'IA abbiano lo stesso livello di protezione delle vittime di danni causati da altre tecnologie. E se è vero che un testo unico e coordinato sarebbe stato preferibile in un'ottica di semplificazione di un sistema già troppo complesso, è anche vero che il campo di possibile applicazione dell'IA è in potenza sterminato. L'IA, infatti, non è una materia, ma un fenomeno. Questo copre oggi qualsiasi aspetto della nostra vita, e non stupisce pertanto che il legislatore abbia deciso di intervenire su più fronti per colmare quello che è percepito come un vuoto normativo.

“EREDITÀ” DIGITALE

Cecilia Trevisi, Sofiae – Solidoro Finulli & Partners

Il progresso tecnologico ha inciso sul modo di concepire il patrimonio di un soggetto soprattutto in ragione del fatto che la vita reale tende sempre più a sovrapporsi alla “vita digitale” fino a confondersi con essa.

Accanto ai beni tradizionali: immobili, mobili, mobili registrati, preziosi e valute, troviamo i nuovi beni digitali: nomi a dominio, password, chiavi di accesso per le piattaforme di e-commerce, username, social account, e-mail (in cui l’asset protetto non è l’account in senso lato ma il contenuto a cui si accede attraverso le credenziali), software, ebooks, musica in formato digitale, documenti informatici, foto, video, arte virtuale e digitale, token (NFT e fungible token).

Si tratta di asset digitali molto eterogenei per cui può risultare complesso e dispersivo cercare di classificarli. Si pensi all’avatar in quanto alter ego digitale, in grado di interagire e relazionarsi in realtà totalmente dematerializzate in cui è possibile perfezionare transazioni economiche aventi contenuto patrimoniale; oppure, più in generale, si pensi agli stessi dati personali, che fino a pochi anni fa erano insuscettibili di essere monetizzati mentre oggi sono qualificati come il nuovo “oro nero”.

Beni che richiedono qualche riflessione più approfondita, non solo per la loro gestione e trasmissibilità nei rapporti inter vivos ma anche per i trasferimenti mortis causa. I problemi più rilevanti, infatti, si pongono nel caso di morte del soggetto (persona fisica) ma lo stesso vale anche nel caso di estinzione di un ente giuridico nel cui patrimonio sono confluiti tali asset senza che vi sia stata alcuna indicazione specifica rispetto alla gestione

o semplicemente alla modalità per accedere a tali contenuti (cosiddetta "morte digitale").

L'obiettivo che si pone tale approfondimento è circoscritto alla sola trasmissione degli asset immateriali nel caso di morte di una persona fisica.

In assenza di specifiche disposizioni testamentarie, chiunque voglia in un primo tempo accedere e, successivamente, gestire o disporre di tali beni (aventi entità patrimoniale e non patrimoniale) è necessario che si munisca di un titolo giudiziale (cautelare ottenuto in via d'urgenza).

«In assenza di specifiche disposizioni testamentarie, chiunque voglia in un primo tempo accedere e, successivamente, gestire o disporre di tali beni (aventi entità patrimoniale e non patrimoniale) è necessario che si munisca di un titolo giudiziale (cautelare ottenuto in via d'urgenza).»

In questi casi, eventuali problemi di transnazionalità (spesso il provider ha sede all'estero) trovano risposta nell'applicazione del "principio della residenza" del de cuius, per cui si applica la legge della "residenza abituale", principio valido sia per i cittadini degli Stati membri dell'Unione sia per i soggetti extracomunitari abitualmente residenti in un Paese UE.

Altre problematiche possono riguardare la "privacy" del soggetto defunto, anche se in realtà si tratta di un falso problema.

È noto che nel Considerando n. 27 del GDPR è stato precisato che il Regolamento non si applica ai dati personali delle persone decedute, demandandosi agli Stati membri la possibilità di introdurre norme riguardanti il trattamento dei dati personali delle persone defunte.

Il D.lgs. n. 101/2018 all'art. 2-terdecies, specificamente dedicato ai temi della tutela post mortem e dell'accesso ai dati personali del defunto, prevede che "i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio o, agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".

La regola generale prevista dal nostro ordinamento, in continuità con la disciplina contenuta nell'art. 9, comma 3, del D.lgs. 196/2003, è quella della sopravvivenza dei diritti dell'interessato in seguito alla morte e della possibilità del loro esercizio, post mortem, da parte di determinati soggetti legittimati all'esercizio dei diritti stessi (in questo senso si è espresso il Tribunale di Milano nell'ordinanza del 2 marzo 2021 e il Tribunale di Roma nell'ordinanza del 10 febbraio 2022).

Tuttavia, come accadeva nella previgente disciplina, il legislatore italiano non ha chiarito neppure nella normativa attualmente in vigore se si tratti di un acquisto mortis causa o di una legittimazione iure proprio, ma si è limitato a prevedere la "persistenza" dei diritti di contenuto digitale oltre la vita della persona fisica, di rettifica e cancellazione (artt. 16 e 17 Reg UE), di limitazione di trattamento (art. 18), di opposizione (art. 21), di portabilità dei dati (art. 20).

«In assenza delle credenziali di accesso a device, social network, e-mail, resta l'alternativa giudiziale; in Italia, ad esempio, è possibile richiedere un provvedimento cautelare che consenta ai soggetti legittimati di avere accesso a tali dati anche mediante consegna delle relative chiavi di accesso.»

Non va, in ogni caso trascurato, che il secondo comma dell'art. 2-terdecies sopra menzionato prevede il diritto di autodeterminazione del soggetto interessato, lasciando a quest'ultimo la scelta di decidere (in vita) se lasciare agli eredi ed ai superstiti legittimati la facoltà di accedere ai propri dati personali (ed esercitare tutti o parte dei diritti connessi) oppure di sottrarre all'accesso dei terzi tali informazioni. L'eventuale volontà dell'interessato di vietare l'esercizio di tali diritti deve risultare in modo non equivoco e deve essere specifica. Il divieto può difatti riguardare l'esercizio soltanto di alcuni dei diritti. Volontà che l'interessato può sempre modificare o revocare.

L'ultimo comma della norma in commento precisa che in ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato, nonché del diritto di difendere in giudizio i propri interessi.

Quindi nel caso in cui un soggetto muoia improvvisamente, senza che gli eredi conoscano le password per accedere ai device del defunto (cellulare, tablet etc.), alle e-mail o alle pagine dei social network anche solo per recuperare il contenuto archiviato nel telefono (foto, video o altro) per ragioni affettive (adducendo ad al cosiddetto "diritto al ricordo"), tali soggetti hanno diritto di accedere ai dati personali del titolare per "ragioni familiari meritevoli di protezione" che giustificano l'accesso ai beni digitali dopo la morte del titolare. Accesso che non può essere precluso, condizionato o limitato dalle condizioni generali di contratto relative al singolo dispositivo o quelle riguardanti specifici social network.

Alcuni social network (Facebook, ad esempio) nel momento dell'accettazione delle condizioni contrattuali che regolano il servizio, indicano all'utente-consumatore la facoltà di scegliere il soggetto che sarà legittimato ad accedere al proprio profilo personale nel caso di morte.

In assenza delle credenziali di accesso a device, social network, e-mail, resta l'alternativa giudiziale; in Italia, ad esempio, è possibile richiedere un provvedimento cautelare che consenta ai soggetti legittimati di avere accesso a tali dati anche mediante consegna delle relative chiavi di accesso. Anche le disposizioni testamentarie possono essere un valido strumento, senza tuttavia dimenticare che la pubblicazione del testamento renderebbe conoscibili le chiavi di accesso.

APPROCCIO RISK-BASED E STRUMENTI LEGAL TECH: STIAMO ANDANDO VERSO UNA COMPLIANCE ANTICIPATORIA FONDATA SULL'INTELLIGENZA ARTIFICIALE?

Giuseppe Vaciago, LT42

Le più importanti normative a livello Europeo (GDPR, Digital Service Act, Digital Market Act) sono tutte "risk-based". Guardando al futuro, è inevitabile ritenere che l'abilità nel creare un modello di gestione del rischio efficace sarà cruciale per fare fronte a queste sfide. L'approccio risk-based assume un ruolo centrale anche nel regolamento sull'Intelligenza Artificiale. La classificazione del rischio passa attraverso vari livelli – inaccettabile, alto, limitato, basso – variabili in base all'AI utilizzata. Questa sorta di "termometro del rischio" porta con sé delle implicazioni giuridiche di notevole portata e una impellente necessità di trovare uno standard di riferimento. Si pensi, ad esempio, al modello forgiato dal NIST nel suo Artificial Intelligence Risk Management Framework[1], o a quello proposto da Oxford (CAP AI[2]) dal "nostro" Luciano Floridi.

Ma cosa intendiamo esattamente per "rischio"? Sebbene possa sembrare una questione banale o pedante, il rischio solitamente è il prodotto di due variabili: la probabilità che si verifichi un evento dannoso e la gravità di tale evento. Da qui deriva il concetto di "rischio inerente", dal quale ci si aspetta una riduzione al "rischio residuo" a seguito dell'implementazione di presidi di controllo adeguati.

Ma è opportuno guardare oltre. Nell'ambito dello Human Rights, Ethical and Social Impact

1 https://www.nist.gov/itl/ai-risk-management-framework

2 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091

Assessment richiesto dal regolamento sull'Intelligenza Artificiale proposto da Alessandro Mantelero nel suo ultimo volume "Beyond Data"[3], le variabili da considerare possono essere ampliate: potremmo considerare non solo la probabilità e la gravità, ma anche il numero di individui potenzialmente toccati dal rischio, definito come "esposizione", nonché lo sforzo necessario per risolvere l'eventuale pregiudizio. Questo ci darebbe una comprensione del rischio più granulare.

«Potremmo quindi immaginare di introdurre ulteriori variabili insieme alla probabilità e alla gravità, come la capacità di un rischio di essere rilevabile, oppure il possibile ammontare della sanzione in caso di una ipotetica violazione. Infine, potrebbe essere il caso di valutare il rischio non solo alla luce delle esperienze passate e dei dati derivanti, bensì contemplando gli scenari futuri.»

È forse proprio in questa direzione che siamo chiamati a muoverci per affrontare la complessità dell'Intelligenza Artificiale. È emblematico il fatto che, secondo una recente analisi di compliance del Regolamento Europeo sui Foundation Models Providers di AI condotta dalla Stanford University[4], solo pochi sistemi attualmente sul mercato rispettano pienamente la normativa europea.

Potremmo quindi immaginare di introdurre ulteriori variabili insieme alla probabilità e alla gravità, come la capacità di un rischio di essere rilevabile, oppure il possibile ammontare della sanzione in caso di una ipotetica violazione. Infine, potrebbe essere il caso di valutare il rischio non solo alla luce delle esperienze passate e dei dati derivanti, bensì contemplando gli scenari futuri.

A New York, nel 1898, il problema principale della città era il letame generato dai 150.000 cavalli che circolavano per le strade ogni giorno. E sembrava fosse impossibile risolvere questo problema, perché invece di ragionare in un'ottica proiettata sul futuro, gli esperti dell'epoca ragionavano senza pensare che potessero esistere tali variabili. Tuttavia, nel

3 *https://link.springer.com/book/10.1007/978-94-6265-531-7*

4 *https://crfm.stanford.edu/2023/06/15/eu-ai-act.html*

1897 nasceva la Model A della Ford, e gli autoveicoli, come è noto, hanno radicalmente cambiato il futuro.

Non dobbiamo, quindi, assolutamente sottovalutare l'importanza del "foresight", intesa come disciplina dell'anticipazione dei possibili futuri al fine di ipotizzare nuovi scenari di rischio su cui inevitabilmente dovremo confrontarci.

Il foresight rappresenta una modalità per anticipare i nuovi livelli di rischio, sfruttando la lungimiranza per anticipare le sfide dell'era dell'AI. In questo scenario molto complesso è lecito chiedersi se l'Intelligenza Artificiale ha il potenziale di trovare strumenti legal and ethical tech per limitare i rischi che essa stessa può generare.

«Se quindi è molto probabile che l'intelligenza artificiale possa aiutare a mitigare i rischi da essa stessa potenzialmente generati, è ovviamente necessaria una continua attività di controllo e gestione da parte dell'uomo per assicurarsi che i sistemi di intelligenza artificiale operino entro i confini legali ed etici desiderati.»

La risposta non può che essere affermativa, anche se i tool sui quali gli esperti di legal tech dovranno confrontarsi dovranno partire dal concetto dell'estensione dell'ambito di competenza: dobbiamo estendere alla sfera etica e sociologica ogni applicazione legal tech attraverso i seguenti strumenti:

- Registrazione e monitoraggio: l'AI può creare e gestire registrazioni dettagliate di tutte le sue operazioni, permettendo un controllo più accurato e continuo. Questo potrebbe includere tracciare l'uso dei dati, la creazione e l'applicazione di modelli di apprendimento automatico, e altri processi chiave;
- Analisi predittiva: l'AI può individuare i rischi prima che questi diventino problematici. Il tutto attraverso l'uso di algoritmi di apprendimento automatico e analisi dei dati. Questo permette di anticipare e mitigare i rischi;
- Elaborazione del linguaggio naturale: gli strumenti di legal/ethical/social tech basati sull'Intelligenza Artificiale possono analizzare grandi volumi di testi legali per identificare problemi, tendenze e cambiamenti nel campo giuridico, aiutando a mantenere aggiornate le policy e le procedure;

- Auto-regolamentazione: attraverso l'apprendimento automatico e la codifica etica, l'AI può essere progettata per auto-regolarsi in base a standard legali ed etici predefiniti;
- Formazione e sensibilizzazione: infine, gli strumenti di AI possono essere utilizzati per formare le persone a comprendere meglio i rischi legali associati alla tecnologia e mitigarli.

Se quindi è molto probabile che l'intelligenza artificiale possa aiutare a mitigare i rischi da essa stessa potenzialmente generati, è ovviamente necessaria una continua attività di controllo e gestione da parte dell'uomo per assicurarsi che i sistemi di intelligenza artificiale operino entro i confini legali ed etici desiderati.

L'uso della tecnologia non deve e non può sostituire il giudizio umano, ma piuttosto funzionare come uno strumento di supporto. Un supporto estremamente valido ed efficace se saremo in grado di governare questo inevitabile processo di cambiamento.

PROTEZIONE DEI SEGRETI COMMERCIALI ATTRAVERSO STRUMENTI LEGAL TECH: IL TRADE SECRETS SCOREBOX

Roberto Valenti, DLA Piper

In una società dominata dalla tecnologia, in cui i dati sono considerati una risorsa primaria, i rischi legati ai segreti commerciali sono aumentati in modo significativo. Un chiaro indicatore è il numero crescente di casi di sottrazione indebita di segreti commerciali avanti i tribunali di tutti i Paesi europei. Pertanto, è sempre più rilevante per le aziende adottare protocolli di sicurezza per proteggere i propri segreti commerciali.

È importante che le organizzazioni imprenditoriali elaborino una solida strategia per la governance dei dati, che va oltre la semplice stesura di policy generalizzate e la creazione di procedure standard. Nell'identificazione e nella tutela dei segreti commerciali, gli strumenti Legal Tech hanno un ruolo fondamentale, ponendosi sia come misure di protezione sia come supporto probatorio per sostanziare le contestazioni di appropriazione indebita.

L'IMPORTANZA DEI SEGRETI COMMERCIALI

La tutela del segreto commerciale è senza limiti temporali, più versatile e potenzialmente più ampia di altri diritti di proprietà intellettuale, e consente di proteggere dati e informazioni che altrimenti non sarebbero coperti dai tradizionali diritti di proprietà intellettuale. Affinché un'informazione possa essere qualificata come segreto commerciale, è necessario che soddisfi specifici requisiti, il più importante dei quali è la segretezza. In Italia, ai sensi dell'art. 98, comma 1, del Codice della Proprietà Industriale, le informazioni, quali know-how, dati commerciali e tecnologici, possono essere protette come segreti

commerciali se: a) non sono facilmente accessibili o generalmente conosciute nel settore di riferimento; b) hanno un valore economico legato alla loro riservatezza; e c) sono soggette a misure adeguate che ne garantiscono la segretezza. Rispetto a quest'ultimo requisito, le imprese devono adottare specifiche misure di protezione, che possono includere strumenti legali, come accordi di riservatezza, misure di sicurezza tecniche e misure organizzative, come la segregazione degli accessi.

«La tutela dei segreti commerciali richiede un approccio multidimensionale, basato sulla classificazione precisa di ciò che costituisce un segreto commerciale rispetto al più ampio ambito delle informazioni riservate. In assenza di un corretto sistema di identificazione dei dati da tutelare, anche le migliori misure di protezione possono risultare insufficienti.»

La tutela dei segreti commerciali richiede un approccio multidimensionale, basato sulla classificazione precisa di ciò che costituisce un segreto commerciale rispetto al più ampio ambito delle informazioni riservate. In assenza di un corretto sistema di identificazione dei dati da tutelare, anche le migliori misure di protezione possono risultare insufficienti.

Pertanto, l'elaborazione di una strategia di difesa dei segreti commerciali deve partire dall'identificazione dei dati qualificabili come segreti commerciali. Ciascuna tipologia di informazione confidenziale presenta difficoltà e possibilità di tutela con soluzioni Legal Tech.

Informazioni proteggibili possono essere quelle tecniche, quali metodologie di produzione, caratteristiche dei prodotti, processi industriali, anche non brevettabili, disegni tecnici, diagrammi, formule e piani tecnici. Possono anche essere rilevanti informazioni commerciali, come piani strategici, elenchi di clienti e fornitori e dati di ricerche di mercato, la cui appropriazione non autorizzata da parte di un competitor potrebbe determinare un significativo svantaggio competitivo per il titolare. Perfino informazioni amministrative, come documenti relativi a certificazioni di qualità, dati finanziari e procedure aziendali interne, possono essere considerate meritevoli di tutela, sussistendo i requisiti di protezione sopra indicati. Infine, nei settori tecnologicamente avanzati sono particolarmente significativi segreti commerciali relativi a software, come codici sorgente

e sequenze operative specifiche.

Una volta identificati, i segreti commerciali devono essere tutelati attraverso adeguate misure di protezione tecniche, contrattuali ed operative, che devono essere soggette ad aggiornamenti periodici. Infatti, deve essere creato un sistema di tutela che si adatta ed evolve, in grado di far fronte agli sviluppi tecnologici e di allinearsi alle best practice più recenti.

L'importanza dei segreti commerciali è aumentata enormemente per effetto della tecnologia. La digitalizzazione consente infatti di processare e conservare enormi quantità di dati, capaci di fornire vantaggi competitivi significativi al titolare di questi dati. Ecco perché è necessario sensibilizzare le imprese verso una più efficiente gestione dei dati aziendali.

«Una volta stabilito il livello effettivo di protezione dei segreti commerciali, gli strumenti Legal Tech possono contribuire a implementare politiche di identificazione e gestione dei segreti commerciali.»

L'impiego di policy e di misure tecniche di protezione può avere un ruolo fondamentale nella tutela dei segreti commerciali. Tuttavia, l'implementazione di tali misure non deve essere considerata in senso statico, ma come processo dinamico, posto in atto in modo rigoroso e con continui controlli di compliance. Le imprese devono anche promuovere corsi di formazione per accrescere la consapevolezza dei dipendenti sull'importanza dei segreti commerciali e sulle conseguenze delle violazioni della riservatezza di tali informazioni. In questo modo, ogni membro dell'organizzazione potrà essere reso responsabile della gestione e dell'utilizzo dei segreti commerciali. Infine, in caso di mancato rispetto dei protocolli di sicurezza deve essere condotta un'indagine immediata per valutare la portata delle violazioni.

IL SUPPORTO DEGLI STRUMENTI LEGAL TECH: TRADE SECRETS SCOREBOX

Come detto, i segreti commerciali sono diventati il fulcro dell'economia digitale: le aziende devono dedicare maggiore attenzione allo sviluppo e all'implementazione di una strategia di protezione di tali asset per garantire il successo e la continuità a lungo termine delle loro attività. Oltre ad offrire un modo semplificato per identificare e classificare le informazioni riservate, gli strumenti Legal Tech consentono di fare fronte ai rischi di sicurezza nei mutevoli contesti tecnologici e normativi, al fine di creare una robusta strategia di protezione dei segreti commerciali, in conformità alle disposizioni vigenti.

Per offrire alle imprese una valutazione dei meccanismi interni di protezione dei segreti commerciali, DLA Piper ha sviluppato Trade Secrets Scorebox, un assessment tool basato sulla normativa dell'Unione Europea.

Questo strumento Legal Tech valuta diversi parametri:

- Livello di consapevolezza all'interno dell'organizzazione: Trade Secrets Scorebox rileva il grado di consapevolezza dei diversi dipartimenti dell'azienda in relazione alla definizione e all'importanza dei segreti commerciali;
- Maturità nella gestione dei segreti commerciali: il tool esamina l'efficacia della tutela dei segreti commerciali e tecnici, evidenziando le aree che necessitano di urgente attenzione;
- Gestione dei segreti commerciali di terzi: Trade Secrets Scorebox valuta la solidità dei protocolli e delle procedure di gestione delle informazioni commerciali e tecniche di terzi, sulla base dell'adeguatezza delle misure contrattuali, delle policy interne e della formazione dei dipendenti;
- Adattabilità rispetto agli sviluppi tecnologici: il tool esamina l'adeguatezza del monitoraggio e dell'aggiornamento delle misure di protezione, alla luce delle innovazioni tecnologiche e i crescenti rischi di cybersecurity.

Dopo aver determinato un punteggio complessivo, il tool fornisce indicazioni per migliorare, rafforzare o riconfigurare la strategia di protezione dei segreti commerciali dell'azienda.

Una volta stabilito il livello effettivo di protezione dei segreti commerciali, gli strumenti Legal Tech possono contribuire a implementare politiche di identificazione e gestione dei segreti commerciali. Aziende come Tangibly Inc. offrono soluzioni SaaS finalizzate a ridurre il rischio di condivisione di segreti commerciali, fornendo (i) strumenti di identificazione di informazioni potenzialmente qualificabili come segreti commerciali; (ii) sistemi di catalogazione delle informazioni che circolano a livello aziendale; (iii) registri degli accessi alle informazioni confidenziali in grado di monitorare la correttezza degli accessi e l'utilizzo in conformità alle policy aziendali.

Come disse Charles Clark alla fine degli anni '90, "the answer to the machine is in the machine itself". Strumenti Legal Tech possono consentire da un lato l'emersione di valori aziendali che le società non sanno nemmeno di avere, e dall'altro fornire gli strumenti per la loro migliore amministrazione.